

## **Свод рекомендаций по противодействию мошенничеству в области электронных платежей**

(Рекомендации по противодействию мошенничеству в области электронных платежей разработаны межведомственной рабочей группой по противодействию мошенничеству в области электронных платежей в соответствии с Планом мероприятий, направленных на противодействие преступным посягательствам в банковской сфере с использованием высоких технологий, утвержденным 29.06.2011 исполняющим обязанности Председателя Правления Национального банка Республики Беларусь Ю.М. Алымовым и 04.07.2011 Министром внутренних дел Республики Беларусь А.Н. Кулешовым)

## Перечень рекомендаций, включенных в настоящий свод:

1. Рекомендации по организации взаимодействия между банками, процессинговыми центрами и органами Министерства внутренних дел в случае выявления мошенничества с банковскими пластиковыми карточками

2. Рекомендации по обеспечению безопасного функционирования программно-технической инфраструктуры банков, ОАО БПЦ, ООО «ВЕБ ПЭЙ» и аналогичных организаций участвующих в обработке интернет-транзакций с использованием банковских пластиковых карточек.

3. Рекомендации для оценки надежности интернет-магазинов, подключаемых белорусскими банками-эквайерами.

4. Рекомендации по противодействию мошенничеству при совершении расчетов в сети Интернет по банковским пластиковым карточкам.

5. Рекомендации банкам по оформлению документов, позволяющих подтвердить ущерб, причиненный резидентам иностранных государств в результате мошенничества в области интернет-эквайринга на территории Республики Беларусь.

## **Рекомендации по организации взаимодействия между банками, процессинговыми центрами и органами Министерства внутренних дел в случае выявления мошенничества с банковскими пластиковыми карточками**

Настоящие Рекомендации регулирует взаимодействие между процессинговыми центрами, банками-участниками платежных систем, подразделениями МВД Республики Беларусь, занимающимися раскрытием преступлений в сфере высоких технологий, и территориальными подразделениями внутренних дел в случае выявления хищений с использованием пластиковых карт или возникновении подозрения в нем.

Для организации взаимодействия стороны определяют ответственных сотрудников и указывают их контактные телефоны и адреса электронной почты, используя специально созданный для этой цели интернет-ресурс Расчетного центра Национального Банка Республики Беларусь.

### **1. Определения, используемые в данных Рекомендациях**

В рамках настоящих Рекомендаций используются следующие определения.

Хищение – действия, направленные на несанкционированное овладение финансовыми средствами, размещенными на карт-счетах клиентов банков-эмитентов пластиковых карт, или причитающимися организации торговли и сервиса (далее – ОТС) за операции по карточкам, и основанные на применении технологии пластиковых карт для доступа к счетам.

Поддельная карта – пластиковая карта, на магнитной полосе, чипе и/или на лицевой и обратной стороне, которой нанесена информация о действительной банковской пластиковой карте, полученная незаконным путем.

«Белый пластик» - вид поддельной карты без признаков платежных систем на лицевой и оборотной сторонах карты.

Перекодированная карта – вид поддельной карты, изготовленной с использованием пластиковой заготовки действительной карты путем

перекодирования данных магнитной полосы или чипа таким образом, что информация на магнитной полосе карты или чипе не соответствует информации нанесенной на лицевую и/или обратную сторону карты.

Скомпрометированная карта – действительная банковская карта, данные которой были скопированы для последующего несанкционированного использования.

Мониторинг – комплекс мероприятий, проводящийся в соответствии с требованиями платежных систем VISA, MasterCard Worldwide, American Express и БелКарт (далее – ПС), с целью выявления операций, несанкционированных держателем карточки, а также операций, проведенных с нарушением правил ПС.

Скимминг – способ хищения данных магнитной полосы карты путем установки на электронный терминал устройства несанкционированно копирующего данные магнитной полосы карты при проведении операции на терминале.

Банк-процессор – банк-резидент, являющийся участником платежных систем и осуществляющий процессинг операций с пластиковыми картами самостоятельно без привлечения процессинговой компании.

Банк-участник – банк-резидент, являющийся участником платежных систем, использующий процессинговую компанию-резидента для осуществления процессинга операций с карточками.

Банк-connector (коннектор) - банк-резидент, являющийся участником платежных систем, использующий процессинговую компанию-нерезидента для осуществления процессинга операций с карточками.

Банк – Банк-участник или Банк-процессор или Банк-connector.

Сервис-провайдер платежей в интернет (СППИ) - процессинговая организация, оказывающая услуги по передаче и обработке транзакций, совершенным в сети интернет с использованием реквизитов БПК.

Процессинговый Центр – процессинговая компания, предоставляющая услуги процессинга операций с карточками Банкам-участникам.

УРПСВТ МВД – подразделение МВД Республики Беларусь, занимающиеся раскрытием преступлений в сфере высоких технологий.

ОВД - территориальные подразделения внутренних дел.

КартЦентр Банка – подразделение Банка, осуществляющее управление и контроль деятельности Банка в сфере обслуживания банковских пластиковых карточек, и взаимодействующее с Процессинговым Центром (если это применимо) и УРПСВТ МВД.

ПСТС – платежно-справочный терминал самообслуживания.

Интернет-магазин – ОТС, выбор товаров или услуг которого осуществляется с помощью интернет-сайта, оплата – путем предоставления держателем карты реквизитов карты.

2. Регламент взаимодействия сторон в случае выявления хищения (подозрения в хищении) в эквайринговой сети Банков

2.1. Изъятие «белого пластика» банкоматом/ПСТС:

- в случае выявления при инкассации банкоматов/обслуживании ПСТС карт типа «белый пластик» ответственный сотрудник Банка, соблюдая требования по сохранению отпечатков пальцев на карте (при физическом контакте с картой необходимо минимизировать площадь соприкосновения карты и рук сотрудника Банка, по возможности стараясь держать карту за торцы), помещает ее в бумажный конверт (или другую емкость) и доставляет в отделение Банка, на обслуживании которого находится банкомат/ПСТС,
- при доставке изъятой карты в отделение Банка, ответственный сотрудник отделения Банка незамедлительно уведомляет КартЦентр Банка о выявленном факте изъятия «белого пластика», сообщает идентификационный код банкомата/ПСТС, номера всех других банковских пластиковых карточек, изъятых в устройстве, описывает внешний вид предположительно поддельной карты,

- ответственный сотрудник КартЦентра Банка-участника в кратчайший срок связывается с Процессинговым Центром, с целью получения сведений указанных в Приложении к данному Порядку,
- Процессинговый Центр (если это возможно) сообщает Банку-участнику информацию о полном номере изъятой карты, операциях, проведенных с ее использованием в устройствах Банка-участника, а также иную информацию, способствующую установлению факта противоправных действий и лиц их совершивших (операции, совершенные до и после операций с изъятой картой), причем перечень передаваемых данных и организация их передачи регламентируются локальными нормативными документами Процессингового Центра и Банка-участника.
- Банк-процессор/Банк-connector самостоятельно выясняет информацию о полном номере изъятой карты, дате и времени ее изъятия, операциях, проведенных с ее использованием, сохраняет материалы системы видеонаблюдения (при ее наличии), а также иную информацию, способствующую установлению факта противоправных действий и лиц их совершивших (операции, совершенные до и после операций с изъятой картой),
- Банк-участник сохраняет материалы системы видеонаблюдения (при ее наличии) по операциям, совершенным с использованием изъятой карты и, если это применимо, по операциям, совершенным до и после операций с изъятой картой,
- в случае получения Банком сведений достаточных для подтверждения факта противоправных действий (однозначное определение номера изъятой карточки) ответственный сотрудник КартЦентра Банка информирует по телефону уполномоченных лиц УРПСВТ МВД и сотрудников отделения Банка о подтвержденном факте использования поддельной карты, а также направляет им по электронной почте сведения об использовании поддельной карты в виде заархивированных графических файлов с паролем,
- в случае отсутствия возможности однозначного определения номера изъятой карточки ответственный сотрудник КартЦентра Банка информирует по телефону уполномоченных лиц УРПСВТ МВД и сотрудников

отделения Банка о подтвержденном факте использования поддельной карты, а также направляет им по электронной почте сведения об использовании поддельной карты в виде заархивированных графических файлов с паролем после проведения исследования карты со считыванием данных магнитной полосы и/или чипа карты,

- ответственный сотрудник отделения Банка обращается в ОВД с письменным заявлением, об использовании пластиковой карты, имеющей признаки подделки, и передает изъятую карту, с целью проведения экспертного исследования на наличие следов пальцев рук, оставленных лицами, использовавшими изъятую карту, а также информацию по операциям с ее использованием и материалы видеонаблюдения,
- передача изъятой карточки Банком в ОВД сопровождается подписанием обеими сторонами акта приема-передачи карточки, один экземпляр акта хранится в Банке, второй экземпляр передается в ОВД вместе с картой,
- в течение 10 банковских дней с момента поступления письменного заявления Банка и изъятой карты в ОВД, ОВД проводит экспертное исследование на наличие следов пальцев рук и передает изъятую карту в отделение Банка, передавшее карту на экспертизу, для последующего считывания полной информации, содержащейся на магнитной полосе (чипе) пластиковой карты,
- порядок передачи изъятой карточки из ОВД в Банк аналогичен порядку передачи карточки из Банка в ОВД и сопровождается актом приема-передачи карточки,
- в случае если у КартЦентра Банка-участника нет возможности считать полные данные магнитной полосы и чипа карты, КартЦентр Банка-участника в течение 3 банковских дней после получения изъятой карты передает ее в Процессинговый Центр, как это описано в локальных нормативных документах Процессингового Центра и Банков, для считывания полной информации содержащейся на магнитной полосе (чипе) пластиковой карты,
- Процессинговый Центр/Банк-процессор/Банк-connector/КартЦентр Банка-участника, имеющий возможность считать полные данные магнитной полосы и чипа карты, проводит исследование карты с целью подтверждения противоправного факта использования

поддельной карты в соответствии с локальными нормативными документами,

- Процессинговый Центр/Банк направляют в банк-эмитент карты, номер которой закодирован на магнитной полосе изъятой карты, запрос с целью подтвердить мошеннический характер операций, совершенных с изъятой картой в эквайринговой сети Банка.

## 2.2. Изъятие перекодированной карты из банкомата/ПСТС

- Банк/Процессинговый Центр осуществляет считывание магнитной полосы (данных чипа) изъятых при инкассации банкоматов/обслуживании ПСТС пластиковых карточек в следующих случаях:
  - отсутствия информации об операциях с номером карты, указанной на лицевой стороне карточки,
  - информация о полном номере карты отсутствует на лицевой стороне карточки,
  - в процессе подготовки отправки карточки банку-эмитенту.
- в случае если при считывании магнитной полосы (чипа) карты Процессинговым Центром/Банком выявлено несоответствие номера карты, закодированного на магнитной полосе, номеру карты, нанесенному на лицевой (оборотной) стороне карты, или записанному в чипе, Процессинговым Центром/Банком проводятся мероприятия по выявлению операций, проведенных с использованием перекодированной карты, а также других сведений, способствующей установлению иных фактов противоправных действий и лиц их совершивших (операции, совершенные до и после операций с перекодированной картой),
- Процессинговый Центр незамедлительно уведомляет КартЦентр Банка-участника о выявленном факте изъятия перекодированной карты, передает сведения, указанные в Приложении к данному Порядку (операции, совершенные до и после операций с изъятой картой, идентификационный код банкомата/ПСТС), организация передачи данных регламентируется локальными нормативными документами Процессингового Центра и Банка-участника,
- Банк сохраняет материалы системы видеонаблюдения (при ее наличии) по операциям, совершенным с использованием перекодированной карты и, если это применимо, по

операциям, совершенным до и после операций с перекодированной картой,

- ответственный сотрудник КартЦентра Банка информирует по телефону уполномоченных лиц УРПСВТ МВД о подтвержденном факте использования поддельной карты, а также направляет им по электронной почте сведения об использовании поддельной карты,
- Процессинговый Центр/Банк-процессор/Банк-connector направляет в банк-эмитент карты, номер которой закодирован на магнитной полосе изъятой карты, запрос с целью подтвердить мошеннический характер операций, совершенных с изъятой картой в эквайринговой сети Банка,
- ответственный сотрудник Банка обращается в УРПСВТ МВД с письменным заявлением, об использовании поддельной пластиковой карты, и предоставляет изъятую карту, а также информацию по операциям с ее использованием и материалы видеонаблюдения.

### 2.3. Обнаружение скиммингового устройства на периферийном оборудовании для работы с пластиковыми картами (банкомате/ПСТС/платежном терминале самообслуживании)

При обнаружении скиммингового устройства на банкомате стороны выполняют следующие действия:

- если информация об обнаружении скиммингового устройства поступила непосредственно в УРПСВТ МВД, ответственный сотрудник УРПСВТ МВД незамедлительно информирует по телефону о данном факте Банк, на обслуживании которого находится данное периферийное оборудование,
- если информация об обнаружении скиммингового устройства поступила в Банк, на обслуживании которого находится данное периферийное оборудование, ответственный сотрудник Банка информирует по телефону о данном факте УРПСВТ МВД после проведения проверки Банком на предмет подтверждения информации,
- если периферийное оборудование, на котором обнаружено скимминговое устройство, находится на обслуживании Банка-участника, ответственный сотрудник Банка-участника также информирует Процессинговый Центр об обнаружении скиммингового устройства,

- Банк, на обслуживании которого находится данное периферийное оборудование, совместно с УРПСВТ МВД принимают решение о возможности снятия скиммингового устройства с периферийного оборудования,
- при наличии информации о дате и времени установки скиммингового устройства Процессинговый Центр/Банк-процессор/Банк-connector формирует отчет об операциях, совершенных на периферийном оборудовании, за период работы скиммингового устройства,
- Процессинговый Центр передает данные об операциях, совершенных на периферийном оборудовании, за период работы скиммингового устройства в Банк-участник по электронной почте с использованием методов защиты информации, рекомендованных Национальным Банком Республики Беларусь (перечень данных указан в Приложении к данному Порядку),
- Банк передает данные об операциях, совершенных на периферийном оборудовании, за период работы скиммингового устройства в УРПСВТ МВД в ответ на официальный запрос УРПСВТ МВД о предоставлении данных (перечень данных указан в Приложении к данному Порядку),
- при отсутствии информации о дате и времени установки скиммингового устройства Процессинговый Центр/Банк-процессор/Банк-connector формирует отчет об операциях, совершенных на периферийном оборудовании, за период с даты последней инкассации банкомата/обслуживания ПСТС/обслуживания платежного терминала самообслуживания, передает данные в УРПСВТ МВД по электронной почте (перечень данных указан в Приложении к данному Порядку),
- Процессинговый Центр/Банк-процессор/Банк-connector передает данные об операциях, совершенных на периферийном оборудовании, за период работы скиммингового устройства в соответствующие банки-эмитенты (перечень данных указан в Приложении к данному Порядку),
- Банки-эмитенты предпринимают действия по изъятию из обращения скомпрометированных карт и их блокировке согласно локальным нормативным документам банков,

- Процессинговый Центр/Банк-процессор/Банк-connector проводит мероприятия в рамках работ по мониторингу по выявлению операций по скомпрометированным картам согласно локальным нормативным документам,
- если скимминговое устройство находится в Банке, Банк, на обслуживании которого находится периферийное оборудование, передает его в УРПСВТ МВД, а также материалы системы видеонаблюдения (при ее наличии) и обращается с письменным заявлением о факте обнаружения скиммингового устройства и возможного несанкционированного копирования информации, находящейся на магнитной полосе карт,
- Процессинговый Центр/Банк-процессор/Банк-connector предоставляет по запросу УРПСВТ МВД сведения об операциях, совершенных с использованием скомпрометированных карт (перечень данных указан в Приложении к данному Порядку).

#### 2.4. Предъявление в ОТС поддельной карты

2.4.1. Если при предъявлении поддельной карты в ОТС, карта изъята из обращения, стороны совершают следующие действия:

- ОТС передает поддельную карту в Банк для проведения исследования карточки,
- Банк-участник согласно локальным нормативным документам передает поддельную карту в Процессинговый Центр для считывания данных магнитной полосы и/или чипа и сканирования лицевой и оборотной стороны карты,
- Процессинговый Центр/Банк-процессор/Банк-connector анализирует данные магнитной полосы/чипа карты, формирует отчет об операциях, совершенных с использованием карты, запрашивает копии карт-чеков по данным операциям, направляет в банк-эмитент факсовое сообщение для подтверждения факта хищения,
- в случае принятия решения Банком-участником об обращении в МВД, Процессинговый Центр по запросу Банка-участника передает изъятую из обращения карту в Банк-участник.

2.4.2. Если информация о факте использования поддельной карты поступила от банка-эмитента по каналам ПС, стороны совершают следующие действия:

- Процессинговый Центр/Банк-процессор/Банк-connector формирует отчет об операциях, совершенных с использованием карты, запрашивает копии карт-чеков по операциям, проводит дополнительное обучение персонала, направленное на предотвращение совершения операций с поддельными/украденными/утерянными картами,
- Процессинговый Центр передает информацию о факте использования поддельной карты, поступившую от банка-эмитента по каналам ПС, Банку-участнику,
- Банк информирует УРПСВТ МВД по телефону о факте использования поддельной карты для оплаты товаров/услуг.

## 2.5. Хищение персонала ОТС

Если у Процессингового Центра/Банка-процессора/Банка-connector в результате мониторинга операций в эквайринговой сети появилось подозрение в совершении хищений при пособничестве сотрудника ОТС, стороны выполняют следующие действия:

- Процессинговый Центр/Банк-процессор/Банк-connector направляют факсовое сообщение в банк-эмитент для подтверждения факта хищения,
- Процессинговый Центр/Банк-процессор/Банк-connector проверяют, оспаривал ли банк-эмитент подозрительные операции,
- Процессинговый Центр/Банк-процессор/Банк-connector запрашивают в ОТС копии карт-чеков по подозрительным операциям,
- Процессинговый Центр передает в Банк-участник анализ результатов мониторинга, информацию об оспаривании операций, сообщение банка-эмитента о мошенническом (преступном) характере операций,
- Банк информирует УРПСВТ МВД по телефону и обращается в ОВД с письменным заявлением о факте хищения при

пособничестве сотрудника ОТС, передает отчет об подозрительных операциях, сообщение банка-эмитента о мошенническом характере операций, копии карт-чеков,

- Банк принимает решение о приостановлении/расторжении договора с ОТС, помещении данных ОТС в базу данных ОТС с подозрительной активностью, направлении в ОТС официального письма с уведомлением о выявленном факте мошенничества, совершенного сотрудником ОТС,
- Банк-участник информирует Процессинговый Центр о решении приостановить/расторгнуть договор с ОТС, и необходимости помещения ОТС в базу данных ОТС с подозрительной активностью,
- УРПСВТ МВД совместно с ОВД проводит оперативно-розыскные мероприятия и следственные действия по факту выявленного хищения.

## 2.6. Хищение в интернет-магазине

Настоящие Рекомендации регулируют взаимодействие между участниками международных платежных систем (процессинговыми центрами, банками-эквайерами, банками-эмитентами), являющимися резидентами Республики Беларусь и не использующих технологию 3-D Secure (в части эмиссии), в случае выявления хищения с использованием реквизитов банковских пластиковых карт (далее - БПК) или возникновении подозрения в нем.

СПШИ и банки-эквайеры (или Процессинговый центр, если эквайером БПК является Банк-участник) обязаны осуществлять внутренний мониторинг операций с использованием реквизитов БПК на предмет совершения мошеннических операций.

Процессинговый Центр/Банки-эквайеры/СПШИ самостоятельно определяют перечень правил и критериев, на основании которых транзакция, совершенная с использованием БПК в сети интернет, является подозрительной.

Если у Банка-эквайера/Процессингового Центра/СПШИ в результате мониторинга операций в сети интернет появилось подозрение в совершении хищений в интернет-магазине или при

получении сообщений банка-эмитента о мошенническом характере операций, совершенных в интернет-магазине, стороны выполняют следующие действия:

- если основанием для предположения факта хищения в интернет-магазине явились результаты мониторинга операций Процессинговый Центр/Банк-эквайер/СПШИ уведомляет банк-эмитент БПК (или Процессинговый центр, если эмитентом БПК является Банк-участник) о подозрении в компрометации БПК и попытке мошенничества по факсу,
- Процессинговый Центр/Банк-эквайер/СПШИ проверяют, оспаривал ли банк-эмитент подозрительные операции.
- По факту получения информации о подозрении в компрометации карты банк-эмитент БПК (или Процессинговый центр, если эмитентом БПК является Банк-участник) связывается с держателем БПК для подтверждения факта совершения им подозрительной транзакции.
- В случае, если держатель БПК не признает данную транзакцию, банк-эмитент (или Процессинговый центр, если эмитентом БПК является Банк-участник) информирует СПШИ и Банк-эквайер о том, что данная транзакция признана мошеннической.
- Банк-эквайер/СПШИ запрашивают в ОТС документы, подтверждающие совершение подозрительных операций,
- Банк-эквайер/СПШИ информирует УРПСВТ МВД по телефону и обращается в ОВД с письменным заявлением о факте хищения в интернет-магазине, передает отчет об операциях, сообщение банка-эмитента о мошенническом характере операций, документы, подтверждающие подозрительные операции.
- Банк-эквайер принимает решение о приостановлении/расторжении договора с ОТС и направлении в ОТС официального письма с уведомлением о выявленном факте мошенничества, и необходимости помещения ОТС в базу данных ОТС с подозрительной активностью,
- Банк-участник информирует Центр о решении приостановить/расторгнуть договор с ОТС, и необходимости помещения ОТС в базу данных ОТС с подозрительной активностью,

- УРПСВТ МВД совместно с ОВД проводит оперативно-розыскные мероприятия и следственные действия по факту выявленного хищения.
3. Регламент взаимодействия сторон в случае выявления хищений с использованием карт Банков
- Процессинговый Центр/Банк получает информацию о хищениях (подделка карты, несанкционированное использование реквизитов карты, использование утерянной/украденной карты) с использованием карт Банка в результате мониторинга операций по картам Банка или от держателя карточки,
  - Банк-участник передает информацию об операциях хищения, совершенных по картам Банка, в Процессинговый Центр для проведения разбирательства, установления точки компрометации данных карты,
  - Процессинговый Центр/Банк-процессор проводит анализ подозрительных авторизаций и транзакций с целью выявить возможную точку компрометации, оценить возможность оспаривания подозрительных операций, запрашивает копии карт-чеков по операциям хищения (за исключением устройств самообслуживания),
  - для выявления точек компрометации Банки обмениваются информацией по выявленным случаям компрометации, используя специально созданный для этой цели интернет-ресурс Расчетного центра Национального Банка Республики Беларусь,
  - если точка компрометации установлена, Процессинговый Центр/Банк-процессор информирует об этом соответствующий банк-эквайер, также Процессинговый Центр информирует Банк-участник.
  - Банк оценивает ущерб, причиненный в результате хищений,
  - в случае причинения ущерба Банку, Банк информирует УРПСВТ МВД по телефону и обращается в ОВД с письменным заявлением о факте хищения по карточке Банка, передает результаты разбирательства, информацию о точке компрометации карты (если она установлена), копии карт-чеков, указывает причиненный ущерб,

- УРПСВТ МВД совместно с ОВД проводит оперативно-розыскные мероприятия и следственные действия по факту выявленного хищения.

#### 4. Конфиденциальность обмена информацией

В процессе взаимодействия стороны обеспечивают полную конфиденциальность информации.

Обмен информацией, содержащей полные номера карт, сроки их действия, данные магнитной полосы и изображения лицевой и оборотной стороны карты, осуществляется только при наличии шифрованного канала связи между сторонами по шифрованному каналу или по открытому каналу с применением шифрования передаваемых данных. Шифрование должно осуществляться в соответствии с Техническими нормативными правовыми актами Республики Беларусь. Если такой канал не установлен между сторонами, информация пересылается по электронной почте в виде архива с паролем отдельно разными сообщениями.

Обмен информацией, содержащей полные номера карт, сроки их действия, данные магнитной полосы и изображения лицевой и оборотной стороны карты, осуществляется только при наличии защищенных каналов связи, в т.ч. криптографическими методами в соответствии с действующими НТПА между сторонами, а также с использованием методов защиты информации, устанавливаемых руководящими документами Национального банка Республики Беларусь, согласованными с ОАЦ при Президенте Республики Беларусь. Если такой канал не установлен между сторонами, информация пересылается по электронной почте в виде архива с паролем отдельно разными сообщениями.

Согласовано:

## Приложение

к Порядку взаимодействия

процессинговых центров,

банков-членов платежных систем и МВД Республики Беларусь

в случае выявления хищений с использованием пластиковых карт

### Перечень данных, передаваемых сторонами в процессе взаимодействия при выявлении мошенничества с пластиковой картой

Тип мошенничества	Передающая сторона	Принимающая сторона	Перечень данных
Изъятие «белого пластика»	Процессинговый Центр	Банк-участник	Операции с изъятой картой типа «белый пластик», операции, совершенные до и после операций с изъятой картой: <ul style="list-style-type: none"><li>- дата, время операции,</li><li>- ID банка-эквайера,</li><li>- MCC код,</li><li>- ID банкомата,</li><li>- номер карты,</li><li>- тип операции,</li><li>- сумма операции,</li><li>- валюта операции,</li></ul>

			- код ответа.
	Банк	МВД	<p>Материалы видеонаблюдения по операциям с изъятой картой, операции с изъятой картой типа «белый пластик», операции, совершенные до и после операций с изъятой картой:</p> <ul style="list-style-type: none"> <li>- дата, время операции,</li> <li>- ID банка-эквайера,</li> <li>- MCC код,</li> <li>- ID банкомата,</li> <li>- номер карты,</li> <li>- тип операции,</li> <li>- сумма операции,</li> <li>- валюта операции,</li> <li>- код ответа.</li> </ul>
Перекодированная карта	Процессинговый Центр	Банк-участник	<p>Идентификационный код банкомата/ПСТС, операции с изъятой картой типа «белый пластик», операции, совершенные до и после операций с изъятой картой:</p> <ul style="list-style-type: none"> <li>- дата, время</li> </ul>

			<p>операции,</p> <ul style="list-style-type: none"> <li>- ID банка-эквайера,</li> <li>- MCC код,</li> <li>- ID банкомата,</li> <li>- номер карты,</li> <li>- тип операции,</li> <li>- сумма операции,</li> <li>- валюта операции,</li> <li>- код ответа.</li> </ul>
	Банк	МВД	<p>Материалы видеонаблюдения по операциям с изъятой картой,</p> <p>идентификационный код банкомата/ПСТС, операции с изъятой картой типа «белый пластик», операции, совершенные до и после операций с изъятой картой:</p> <ul style="list-style-type: none"> <li>- дата, время операции,</li> <li>- ID банка-эквайера,</li> <li>- MCC код,</li> <li>- ID банкомата,</li> <li>- номер карты,</li> <li>- тип операции,</li> </ul>

			<ul style="list-style-type: none"> <li>- сумма операции,</li> <li>- валюта операции,</li> <li>- код ответа.</li> </ul>
Обнаружение скиммингового устройства	Процессинговый Центр	Банк-участник	<p>Операции, совершенные за время работы скиммингового устройства:</p> <ul style="list-style-type: none"> <li>- дата, время операции,</li> <li>- ID банка-эквайера,</li> <li>- ID банкомата,</li> <li>- номер карты,</li> <li>- тип операции,</li> <li>- сумма операции,</li> <li>- валюта операции,</li> <li>- код ответа.</li> </ul>
	Банк	МВД	<p>Операции, совершенные за время работы скиммингового устройства:</p> <ul style="list-style-type: none"> <li>- дата, время операции,</li> <li>- ID банка-эквайера,</li> <li>- ID банкомата,</li> <li>- номер карты,</li> </ul>

			<ul style="list-style-type: none"> <li>- тип операции,</li> <li>- сумма операции,</li> <li>- валюта операции,</li> <li>- код ответа.</li> </ul>
	Процессинговый Центр/Банк- процессор	Банки- эмитенты	<p>Операции, совершенные за время работы скиммингового устройства:</p> <ul style="list-style-type: none"> <li>- дата, время операции,</li> <li>- ID банкомата,</li> <li>- номер карты.</li> </ul>
Хищение с использование карт Банков	Процессинговый Центр/Банк- процессор	Банк-эквайер	<ul style="list-style-type: none"> <li>- ID точки компрометации,</li> <li>- даты операций,</li> <li>- номера скомпрометированны карт.</li> </ul>

**Рекомендации по обеспечению безопасного функционирования программно-технической инфраструктуры банков, ОАО БПЦ, ООО «ВЕБ ПЭЙ» и аналогичных организаций участвующих в обработке интернет-транзакций с использованием банковских пластиковых карточек.**

1. Банкам эквайерам и организациям, участвующим в обработке интернет-транзакций с использованием банковских пластиковых карточек, выполнять требования международных платежных систем Visa и MasterCard, в том числе ежегодно проходить PCI DSS аудит;
2. В соответствии с Указом Президента Республики Беларусь от 1 февраля 2010 г. № 60 организациям, участвующим в обработке интернет-транзакций с использованием банковских пластиковых карточек, размещать все объекты программно-технической инфраструктуры, в том числе коммуникационное оборудование, программно-аппаратные комплексы обеспечивающие безопасную обработку интернет-транзакций по технологии VERIFIED by VISA и MasterCard SecureCode, оборудование для осуществления обработки и хранения информации по операциям с БПК, на территории Республики Беларусь;
3. Организациям, участвующим в обработке интернет-транзакций с использованием банковских пластиковых карточек осуществлять хранение всей имеющейся информации, связанной с операциями с использованием БПК в течение не менее восемнадцати месяцев с момента осуществления таких операций на территории Республики Беларусь;

## Рекомендации для оценки надежности интернет-магазинов, подключаемых белорусскими банками-эквайерами

Банки-эквайеры при подписании договоров эквайринга с организациями торговли и сервиса, осуществляющими реализацию товаров (работ, услуг) через интернет (далее – интернет-магазины), осуществляют контроль за соблюдением требований международных платёжных систем в части требований к информации, размещенной на сайтах Интернет-магазинов.

Для целей настоящих Рекомендаций применяются термины и их определения в значениях, установленных законами Республики Беларусь "О защите прав потребителей" от 09.01.2002 №90-З (ред. от 08.07.2008) и "О торговле" от 28.07.2003 №231-З, а также следующие термины и их определения:

покупатель – физическое лицо, имеющее намерение заказать или приобрести либо заказывающее, приобретающее или использующее товары исключительно для личных, бытовых, семейных, домашних и иных нужд, не связанных с осуществлением предпринимательской деятельности;

продавец – организация, ее филиал, представительство, иное структурное подразделение, расположенное вне места нахождения организации, индивидуальный предприниматель, реализующие товары покупателю по договору розничной купли-продажи;

интернет-магазин – сайт, содержащий информацию о товарах, продавце, позволяющий осуществить выбор, заказ и (или) приобретение товара.

### Требования к сайтам Интернет-магазинов.

Ниже приведены требования к магазинам, принимающим банковские пластиковые карты(далее БПК) через интернет, с учетом требований Правил осуществления розничной торговли по образцам и требований международных платёжных систем (Visa International Service Association, MasterCard WorldWide) к оформлению интернет-сайтов.

В случае несоответствия требованиям, сайт Интернет-магазина должен быть доработан.

## 1. Сайт Продавца должен содержать следующие разделы:

1.1. Справочная информация об Интернет-магазине, в том числе наименование (фирменное наименование), а если продавцом является индивидуальный предприниматель, - фамилию, собственное имя, отчество, а также режим работы. Обязательным условием является наличие страны, юридического и фактического адреса (адрес не может быть до востребования), а также контактных телефонов, по которым покупатель может связаться со службой поддержки интернет-магазина, информация о номере специального разрешения (лицензии), сроке его действия, государственном органе или государственной организации, выдавших это специальное разрешение (лицензию), если вид деятельности, осуществляемой продавцом, подлежит лицензированию.

### 1.2. информация о товарах (работах, услугах):

наименование товара;

цены на товары (работы, услуги), комплектность;

полнота описания потребительских характеристик продаваемых товаров (услуг), включая фотографии или другие информационные материалы, содержащие полную, достоверную и доступную информацию, характеризующую предлагаемый товар (работу, услугу);

гарантийный срок, если он установлен;

наименование (фирменное наименование), место нахождения изготовителя (продавца), а также при наличии импортера, представителя, ремонтной организации, уполномоченной изготовителем (продавцом, поставщиком, представителем) на устранение недостатков товара и (или) его техническое обслуживание; если изготовителем (продавцом, импортером, представителем, ремонтной организацией) является индивидуальный предприниматель - фамилию, собственное имя, отчество индивидуального предпринимателя;

сведения о сроке доставки товара, цене и об условиях оплаты доставки товара.

1.3. Указание на нормативные документы, устанавливающие требования к качеству товара (для товара, выпускаемого по таким нормативным документам); гарантийный срок, если он установлен.

1.4. Описание процедуры заказа товара/услуги с обязательным ознакомлением с ней держателя БПК;

1.5. Указание способа оплаты товара/услуги по БПК и валюты операции;

1.6. Информация по доставке товара/услуги, такая как сроки, способы, а также любая другая информация, необходимая для получения ясного представления о доставке товара (услуги) после оплаты с использованием БПК с обязательным ознакомлением с ней держателя БПК;

1.7. Экспортные ограничения по доставке товара/услуги (если существуют);

1.8. Рекомендации держателям карточек сохранять копии записей операций;

1.9. Описание процедур возврата денежных средств, предоставления взаимозаменяемых товаров/услуг, обмена товаров/услуг и т.п. при отказе от товара/услуги с обязательным ознакомлением с ней держателя БПК. В случае если такие процедуры интернет-магазином не предусмотрены, то он обязан информировать об этом на своих страницах.

1.10.. Логотипы платежных систем и банковских пластиковых карточек, принимаемых в интернет-магазине в качестве средства платежа, перечень которых согласован между Банком и Организацией торговли и сервиса, в т.ч. логотипы платежных систем Verified by VISA и MasterCard SecureCode.

2. Организациям торговли и сервиса, работающим в сфере игорного бизнеса (включая ставки на мероприятия и пари), необходимо иметь на сайте следующую информацию:

2.1. "Игорный бизнес через интернет может являться незаконным с точки зрения юрисдикции страны, в которой Вы находитесь. Если это так, Вы не можете произвести платеж по Вашей банковской карте". ("The statement "Internet Gambling may be illegal in the jurisdiction in which you are located; if so, you are not authorized to use your payment card to complete this transaction");

2.2. Заявление о том, что владелец БПК несёт ответственность за невыполнение законов своей страны относительно игр на деньги в

интернет (Cardholder's responsibility to know the laws concerning online gambling in his country of domicile);

2.3. Заявление о том, что пользоваться услугами данного сайта могут только люди старше 18 лет;

2.4. Правила игры (игр), ставок;

2.5. Порядок и сроки выплаты выигрышей;

2.6. Правила возврата платежей.

3. Дополнительные требования:

3.1. Сайт интернет-магазина не должен располагаться на бесплатных серверах, предоставляющих услуги хостинга (например, narod.ru);

3.2. Реквизиты БПК не должны приниматься на страницах интернет-магазина, а при оплате БПК покупатель должен переадресовываться на защищенную страницу Банка-эквайера или процессинговой системы (IPSP);

3.3. Все страницы, которые связаны с работой интернет-магазина, должны находиться под единым доменным именем.

3.4. Интернет-магазин имеет право взимать дополнительно к цене товара (работ, услуг) плату за обработку заказа и/или доставку, при условии, что данная плата также взимается в случае оплаты другими средствами платежа и/или в другой форме (например, оплата наличными денежными средствами).

3.5. Продавец обязан осуществлять контроль за получением заказов своими покупателями.

4. Банк-эквайер имеет право отказать в заключении договора эквайринга или расторгнуть договор, если Продавец:

4.1. в интернет-магазине осуществляет реализацию:

- изделий из драгоценных металлов и драгоценных камней;
- пиротехнических изделий;
- лекарственных средств;
- биологически активных добавок к пище, подлежащих реализации только через аптеки;

- ветеринарных средств;
  - оружия и патронов к нему
  - товаров (работ, услуг), запрещенных действующим законодательством Республики Беларусь, а также категорий «развлечения «для взрослых» («Adult Entertainment», секс-шоп, женский и мужской эскорт).
- 4.2. хранит в каком-либо виде следующие данные:
- номера банковских пластиковых карточек в незашифрованном виде;
  - CVV2/CVC2;
  - сроки действия банковских пластиковых карточек;
  - пароли, используемые при аутентификации держателей банковских пластиковых карточек с использованием следующих методов:
    - Verified By Visa;
    - MasterCard SecureCode.
- 4.3. прямо или косвенно ограничивает покупателя (заказчика) при выборе товаров (работ, услуг).
- 4.4. позволяет разбивать стоимость одной покупки или услуги на несколько частей с последующей их оплатой банковской пластиковой карточкой в виде отдельных операций.
- 4.5. позволяет принимать другие средства и/или формы платежа для оплаты части стоимости одной покупки или услуги (например, одна часть стоимости покупки оплачена банковских пластиковых карточек, другая часть наличными денежными средствами).
- 4.6. Осуществляет возврат денежных средства покупателю (заказчику) в наличной форме (полностью или частично) по ранее совершенным операциям с использованием банковских пластиковых карточек.
- 4.7. Размещает на интернет-сайте информацию, содержащую:
- оскорбительные выражения и предложения, нецензурные высказывания;
  - порнографические материалы;
  - рекламу интимных услуг;
  - ссылки или баннеры подозрительных веб-сайтов (например, веб-сайтов «для взрослых» и т.п.).

## **Рекомендации по противодействию мошенничеству при совершении расчетов в сети интернет по банковским пластиковым карточкам**

Описание процедуры предотвращения мошеннических операций (микроплатеж - двух факторная аутентификация).

При совершении оплаты с использованием иностранной БПК Платежный сервер осуществляет ON-LINE авторизацию с использованием данной БПК на случайную сумму от 0,5 до 2 USD (микроплатеж).

Держатель БПК должен узнать сумму микроплатежа в банке-эмитенте БПК и ввести сумму микроплатежа для подтверждения совершения основной оплаты в течение 1-го часа.

Если сумма микроплатежа совпадает с введенной держателем БПК суммой, валидация карты считается успешной, Платежный сервер осуществляет ON-LINE авторизацию на основную сумму оплаты и формирует операцию отмены по микроплатежу.

В случае, если держатель БПК неправильно ввел сумму микроплатежа три раза или не ввел ее в течение 1-го часа, Платежный сервер формирует операцию отмены по микроплатежу и не осуществляет ON-LINE авторизацию на основную сумму оплаты.

**Рекомендации банкам по оформлению документов, позволяющих подтверждать ущерб, причиненный резидентам иностранных государств в результате мошенничества в области интернет-эквайринга на территории Республики Беларусь“**

Проект набора документов, позволяющих подтверждать ущерб, причиненный резидентам иностранных государств в результате мошенничества в области интернет-эквайринга на территории Республики Беларусь.

1. Оригинальное заявление в правоохранительные органы Республики Беларусь физического лица-держателя карточки, в котором будет отражено, что оно просит осуществить расследование, так как не осуществляло конкретных операций с карточкой в определенных точках в определенное время;
2. Заявление (копия либо электронная копия) физического лица-держателя карточки, в котором будет отражено, что оно не осуществляло конкретных операций с карточкой в определенных точках в определенное время (как правило, с таким обращением держатель обращается в банк-эмитент);
3. Заявление банка-эмитента с отражением вышеуказанных сведений об оспоренных транзакциях (дата, время и место операции, торговая точка, ее тип и месторасположение, сумма и валюта операции, приобретаемый товар или имущество, номер карточки, банк-эмитент, данные держателя, сведения, оставленные при осуществлении транзакции (IP-адреса, адреса электронной почты, контактные телефоны и данные, звукозапись разговоров при покупке), а также и иные данные, которые могут изобличить преступника);
4. Переписка с банком-эмитентом с отражением сведений, указанных в пунктах 1-3;
5. Заявление белорусского банка, к которому могут прилагаться документы и сведения, отраженные в пунктах 1-3;
6. Заявление представителя платежной системы о совершенных мошеннических операциях, в котором будут отражены все сведения из пункта 3 (с приложением документов, подтверждающих полномочия

представителя платежной системы и отражающих Правила системы по мошенническим операциям);

7. Заявление белорусского банка, в котором могут быть описаны обстоятельства совершенных мошеннических операций (с констатацией такого факта), с отражением всех сведений (путем выписок из Правил системы) относительно функционирования платежных систем, формирования базы мошеннических операций, полномочий банка относительно доступа к данной базе и предоставления сведений базы в правоохранительные органы.