



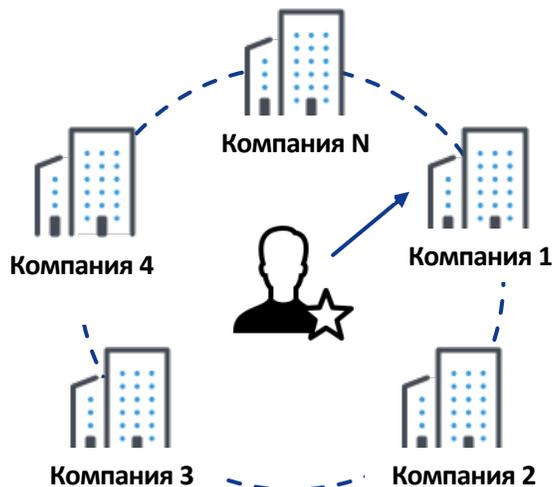
КОДЕКС ЭТИКИ
ИСПОЛЬЗОВАНИЯ
ДАННЫХ

БЕЛАЯ КНИГА

СВОД ЛУЧШИХ ПРАКТИК
В СФЕРЕ ДОБРОСОВЕСТНОГО ИСПОЛЬЗОВАНИЯ ДАННЫХ

УДАЛЕННАЯ ИДЕНТИФИКАЦИЯ

1. Пользователь проходит полную идентификацию в Компании 1. Пользователю присваивается уникальный идентификатор



2. Пользователь, прошедший идентификацию в Компании 1, обращается за сервисом в Компанию 2



3. Компания 2, с согласия Пользователя, осуществляет сверку идентификаторов с Компанией 1, устанавливает клиента* – и оказывает услугу



Положительный эффект от внедрения практики:

- Пользователь получает «бесшовный доступ» к сервисам и экономит своё время
- Компании повышают доступность услуг для клиентов за счёт снятия входного барьера
- Компании экономят время на обслуживание
- Решение обеспечивает безопасность клиентов

Пример:

Пользователь обращается, например, к сервису государственных услуг. Производится полная идентификация Пользователя, то есть осуществляется идентификация, обработка и сохранение данных о Пользователе

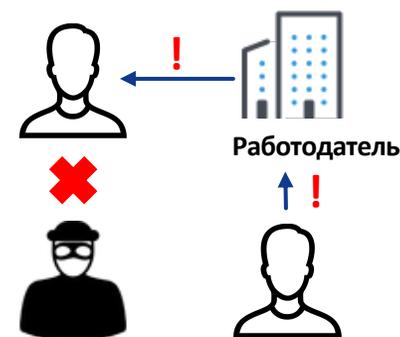
Пользователю присваивается уникальный идентификатор. При обращении Пользователя, например, на интернет-площадку, эта интернет-площадка не осуществляет идентификацию, а с согласия Пользователя, устанавливает его по уникальному идентификатору, осуществив сверку идентификаторов с сервисом государственных услуг

* - практика не распространяется на ситуации обязательной идентификации, определенные федеральным законом 115-ФЗ. Важно отметить, что в рамках этой практики Компания 1 при проведении идентификации не вправе обогащать свои данные. Ее задача лишь оказать услугу по идентификации.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ РОДСТВЕННИКОВ СОТРУДНИКОВ ПРИ ПРОВЕРКАХ В РАМКАХ СОБЛЮДЕНИЯ АНТИКОРРУПЦИОННОГО ЗАКОНОДАТЕЛЬСТВА

При возможном возникновении конфликта интересов или оценки работодателем возможности коррупционных действий, работник сообщает работодателю данные о родственниках – потенциальных участниках такого конфликта или таких действий

Работодатель для оценки ситуации обрабатывает персональные данные родственников без получения от них согласия



Положительный эффект от внедрения практики:

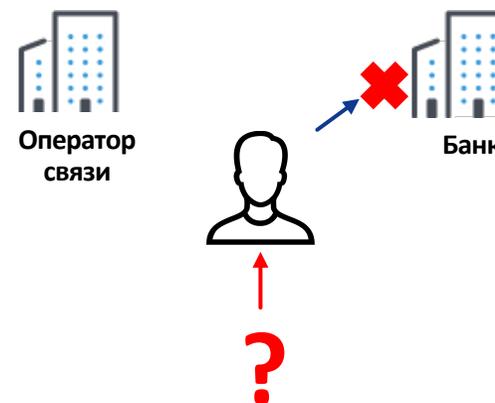
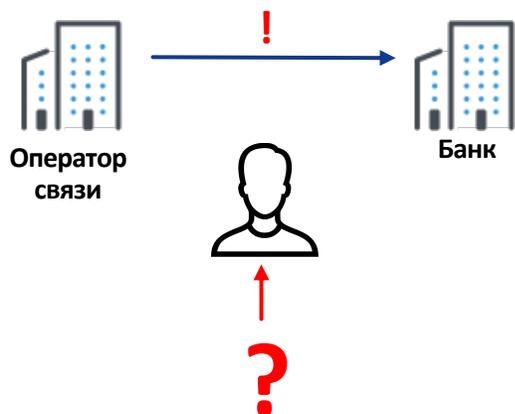
Работодатель сможет должным образом оценить наличие конфликта интересов, принять адекватные меры по предотвращению или урегулированию конфликта интересов. Тем самым добросовестно исполнить антикоррупционные требования законодательства

Пример:

При приеме или переводе на новую работу сотрудник указывает сведения о ФИО и трудовой деятельности своих родственников, которая может быть расценена как потенциальный конфликт интересов. Для оценки наличия или отсутствия конфликта интересов работодатель осуществляет проверку, используя полученную информацию, не запрашивая у поименованных родственников согласия на обработку полученных персональных данных

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ С ЦЕЛЮ ЗАЩИТЫ СЧЕТОВ КЛИЕНТОВ

Для противодействия мошенничеству путем имитации входящего звонка от кредитной организации операторы связи в момент поступления такого звонка автоматически связываются с кредитной организацией для подтверждения реальности звонка



Положительный эффект от внедрения практики:

- Защита клиентов от противоправных действий третьих лиц в удаленных каналах, снижение потерь клиентов от мошеннических действий
- Снижение операционных и репутационных рисков кредитных организаций, повышение безопасности дистанционных каналов обслуживания

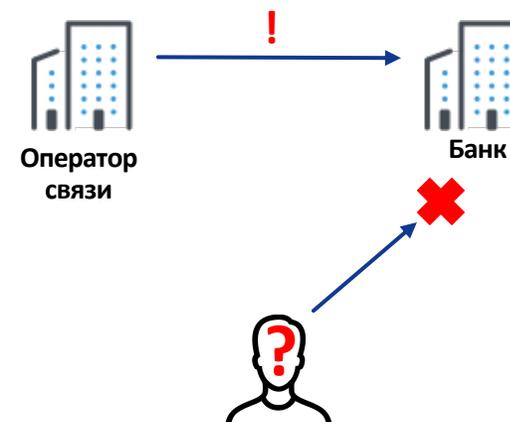
Пример:

При заключении договора обслуживания с кредитной организацией клиент/абонент соглашается на **передачу своих персональных данных кредитной организацией оператору сотовой связи**

В момент звонка с подозрительного номера абоненту оператор передает эту информацию в кредитную организацию. Если по счетам клиента/абонента производятся сомнительные операции, то кредитная организация их блокирует до момента их подтверждения клиентом/абонентом

ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ НА ФИНАНСОВОМ РЫНКЕ

Прямое взаимодействие кредитных организаций и операторов сотовой связи для получения сведений, связанных с подозрительными событиями (смена сим-карты, переадресация вызова, прекращение договора абонентского обслуживания, смена пользовательского устройства и пр.) в режиме онлайн



Положительный эффект от внедрения практики:

- Защита клиентов от противоправных действий третьих лиц в удаленных каналах, снижение потерь клиентов от мошеннических действий
- Снижение операционных и репутационных рисков кредитных организаций, повышение безопасности дистанционных каналов обслуживания

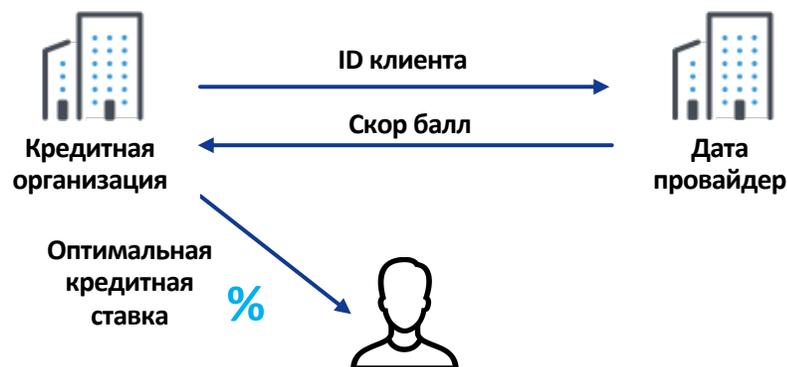
Пример:

При заключении договора обслуживания с кредитной организацией клиент/абонент соглашается на передачу своих данных оператором сотовой связи кредитной организации.

При совершении подозрительного события, например, при смене пользовательского устройства клиента/абонента, оператор отправляет данную информацию в кредитную организацию. Кредитная организация приостанавливает операции по счетам клиента/абонента до момента идентификации лица, их совершающего

СКОРИНГ КЛИЕНТОВ ПРИ ОБРАЩЕНИИ ЗА КРЕДИТОМ

При обращении клиента за кредитом кредитная организация, с согласия клиента, вправе обратиться к провайдерам аналитических услуг (например, сотовому оператору) для оценки вероятности возврата кредита данным клиентом. Для идентификации клиента провайдером используется уникальный идентификатор – номер мобильного телефона, адрес электронной почты и др. Провайдер производит оценку вероятности возврата кредита на основании собственных данных и математических моделей. Целью обращения является уточнение собственной оценки банка для предложения клиенту максимально низкой возможной ставки.



Положительный эффект от внедрения практики:

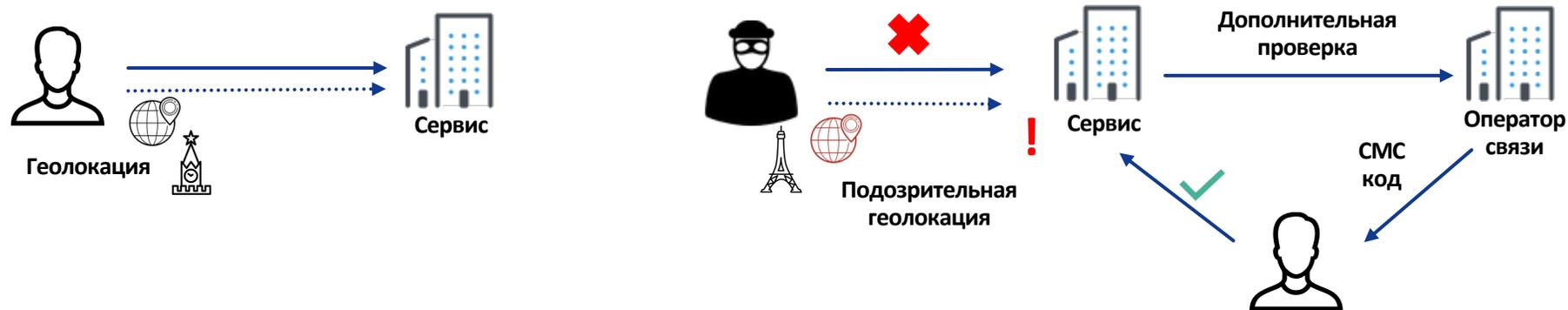
- Удобство: в большинстве случаев клиенту не нужно собирать большой комплект документов для оформления кредита (справка о доходах, копия трудовой книжки и др.). При наличии согласия клиента, всю необходимую для принятия решения информацию кредитная организация получит у провайдеров аналитических услуг.
- Скорость: решение по кредиту, как правило, клиент получает за несколько минут, т.к. кредитная организация в online режиме получает всю необходимую информацию, оценивает ее и принимает решение.
- Более привлекательные условия по кредиту: чем больше у кредитной организации информации по клиенту, тем точнее она может оценить уровень риска по кредиту и предложить для клиента выгодные условия.
- Взвешенное решение: при принятии решения на основе различных скорингов оценивается возможность заемщика по погашению кредита без ущерба для бюджета семьи

Пример:

Клиент обращается в кредитную организацию за кредитом, заполняет заявку указывая свои данные, включая номер мобильного телефона и другие идентификаторы. Кредитная организация просит клиента дать согласие на обработку его персональных данных, а также на передачу их 3-му лицу – провайдеру аналитических услуг. Кредитная организация обращается к провайдеру аналитических услуг и просит предоставить вероятность возврата кредита клиентом на основании его идентификатора. Кредитная организация рассчитывает минимально возможную процентную ставку по кредиту для клиента на основании собственной риск политики и рассчитанного провайдером аналитических услуг скор балла.

СИСТЕМА ДОПОЛНИТЕЛЬНОЙ ВЕРИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ С ЦЕЛЮ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ

При авторизации из подозрительной локации (новая и/или значительно отдаленная) дополнительно запрашивается ввод кода, который отправляется пользователю по дополнительному каналу связи (например, в СМС-сообщении).



Положительный эффект от внедрения практики:

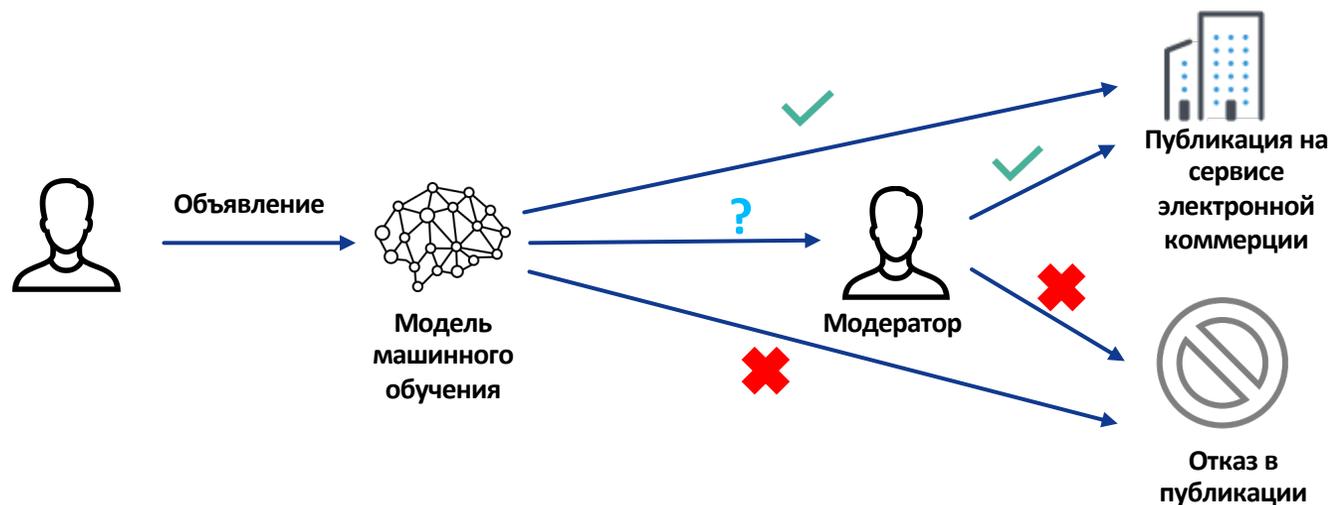
- Дополнительная защита персональных и конфиденциальных данных пользователя от возможного взлома системы из-за дискредитации логина и пароля пользователя в результате фишинга или социальной инженерии, или любого другого метода взлома.
- Снижение риска появления недовольства и материальных претензий к сервису от пользователя взломанного аккаунта.

Пример:

При первой авторизации в сервисе сохраняются данные о геолокации пользователя. В дальнейшем, если авторизация происходит из подозрительной локации, то клиенту по дополнительному каналу связи направляется код, который вводится в специальном поле верификации. Допускается использование иных способов верификации добросовестной пользовательской активности. Подозрительная локация – та, которая отличается от первоначального местоположения, где проходила авторизация пользователя (а также находится на большом расстоянии от него – например, в другой области).

ПРЕДОТВРАЩЕНИЕ РАЗМЕЩЕНИЯ ОБЪЯВЛЕНИЙ С ЗАПРЕЩЕННЫМИ ТОВАРАМИ И УСЛУГАМИ, И ДУБЛИРОВАНИЯ ОБЪЯВЛЕНИЙ

При размещении объявления происходит оценка загруженного контента, в том числе с использованием автоматической обработки данных (текст объявления, хеши ip адресов и cookie, хеши изображений) алгоритмами машинного обучения, затем выносится вердикт о допуске объявления, его отклонении, или необходимости ручной модерации, по результатам которой модель дообучается.



Положительный эффект от внедрения практики:

- Содействие соблюдению законодательства. Ограничение торговли запрещенным товаром
- Защита пользователей от неприемлемого контента
- Повышение удобства сервиса благодаря фильтрации дублирующих объявлений

Пример:

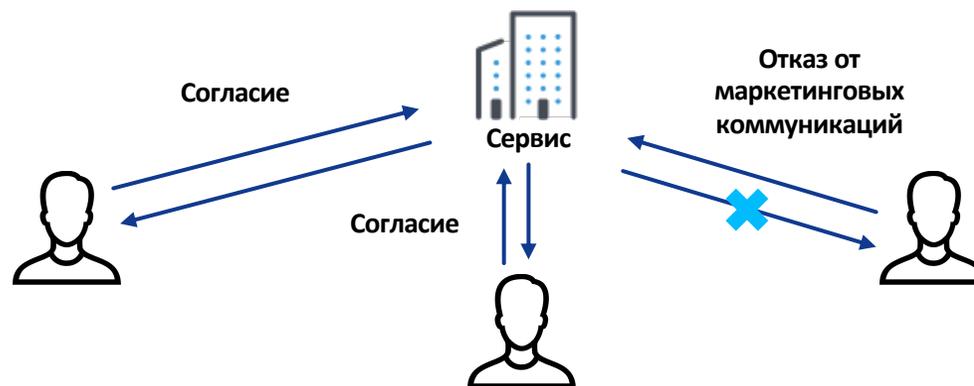
Пользователь электронной доски объявлений размещает объявление с запрещенным товаром или услугой, либо создает дублирующее объявление.

При публикации, многие факторы объявления, в том числе данные пользователя и параметры объявления (хеши ip адресов и cookie, тексты объявлений, а также хеши изображений) проверяются на соответствие законодательству и политике сервиса различными методиками, включая модели машинного обучения, и выносится вердикт соответствия.

По результатам проверки, объявление либо допускается к публикации, либо отклоняется, либо направляется на ручную проверку модератором, если нет достаточной уверенности в корректности автоматизированного вердикта. По результатам ручной модерации проводится обновление модели.

МЕХАНИЗМ ПОЛУЧЕНИЯ И ОБРАБОТКИ ОБРАЩЕНИЙ ЛИЦ, ОТКАЗАВШИХСЯ ОТ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ И/ИЛИ ОТ ОБРАБОТКИ СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъект персональных данных может потребовать у оператора остановить обработку своих данных таким оператором с использованием его информационных систем и баз данных, после чего незамедлительно прекращается любое использование данных для коммуникации, а также в маркетинговых, аналитических и любых иных целях (за исключением случаев, когда у оператора есть иные законные основания такой обработки).



Положительный эффект от внедрения практики:

- Защита прав граждан по защите от нежелательной коммуникации и нежелательного использования своих данных
- Сокращение случаев нарушения законодательства по работе с персональными данными
- Формирование позитивного отношения к компании и ее продуктам со стороны потребителя.

Пример:

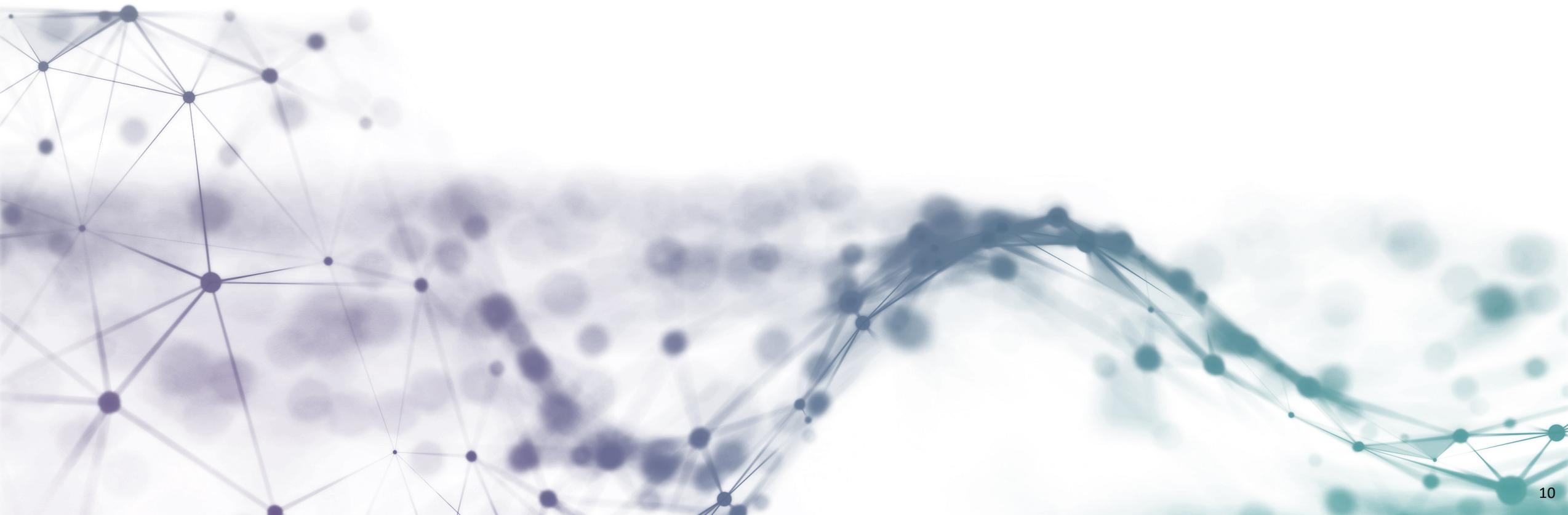
Компании – операторы персональных данных могут обрабатывать и использовать лишь те данные, на обработку которых дано прямое согласие субъекта данных или есть иные законные основания такой обработки, согласно законодательству РФ.

При проведении маркетинговых коммуникаций потребителям предлагаются сценарии отказа от них.

При отказе потребителя от получения рекламных сообщений учитывается это обращение, незамедлительно прекращается направление потребителю таких сообщений посредством информационных систем, посредством собственных каналов коммуникации.

При этом, каждой компанией ведется учет лиц, отказавшихся от получения рекламных сообщений.

ПРИЛОЖЕНИЕ 1



1. УДАЛЕННАЯ ИДЕНТИФИКАЦИЯ

Подробное описание практики

Для обеспечения большей достоверности на практике используются многофакторные модели аутентификации. Лицо считается установленным, если получен положительный результат сопоставления предоставленных субъектом идентификаторов с факторами аутентификации, которыми обладает или может получить из доверенного источника (информационные системы банков, операторов связи, ГИС, «цифровой профиль гражданина» и пр.) идентифицирующее лицо.

Целесообразно использование принципа технологической нейтральности: способы идентификации должны быть равнозначными и влечь равные правовые последствия. Во-первых, в законодательстве не существует каких-либо устоявшихся и обоснованных критериев, по которым использование идентификатора может быть привязано к конкретным правоотношениям. Во-вторых, в соответствии с принципом диспозитивности и свободы участников гражданско-правовых отношений нельзя ограничивать стороны последних в использовании тех или иных идентификаторов, которые они посчитают возможным.

Цифровые способы идентификации могут использоваться в любых правоотношениях, если иное не запрещено законом или соглашением сторон.

В случаях, предусмотренных федеральными законами или принятыми в соответствии с ними иными нормативными правовыми актами, либо соглашением сторон, при дистанционном выражении воли физическим или юридическим лицом с помощью электронных или иных аналогичных средств такое физическое или юридическое лицо может быть установлено путем применения одного из идентификаторов.

Не допускается сбор избыточных персональных данных под видом идентификации, а также навязывание процедуры идентификации в сервисах, реализующих услуги/товары, необходимость в проведении которой, ввиду специфики самого сервиса и/или требований закона, отсутствует.

2. ОБРАБОТКА ДАННЫХ РОДСТВЕННИКОВ

Подробное описание практики

Ряд федеральных законов (например, федеральный закон «О противодействии коррупции»), содержит требования о предоставлении гражданами персональных данных своих родственников в целях предотвращения коррупции, обеспечения достоверности отчетности и пр. Таким образом, информация поступает ее получателю не от самого родственника, а от третьего лица – потенциального кандидата на должность и пр.

Добросовестной практикой целесообразно считать обработку персональных данных организацией-получателем этих данных и лицом, предоставляющим сведения о родственниках, с связи с обработкой таких данных в силу исполнения ими обязанностей, предусмотренных законодательством РФ, а также в связи с обработкой персональных данных, подлежащих обязательному раскрытию или опубликованию, или обработкой персональных данных в общественном интересе.

На основании п. п. 2, 7, 11 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» ДОПУСТИМО не требовать от работников и иных лиц предоставления согласия субъекта персональных данных при направлении в организацию сообщений, уведомлений и т.п., содержащих данные третьих лиц, в рамках противодействия коррупции и управления конфликтом интересов.

3. ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ С ЦЕЛЬЮ ЗАЩИТЫ СЧЕТОВ КЛИЕНТОВ

Подробное описание практики

Операторами связи разработан системный подход по предотвращению данного вида мошенничества с подменой номеров кредитных организаций. Универсальное технологическое решение предполагает интеграцию кредитных организаций по API и предоставление перечня номеров клиентов, по которым необходима нотификация по различным событиям.

Перечень событий может быть индивидуально согласован с кредитной организацией, например, нотификация по вызовам, совершенным с официальных номеров банка, вызовам с номеров, визуально похожих на номера банка, вызовам с номеров, используемых мошенниками для обзвона клиентов банка.

Операторы связи на своей стороне проводят аналитику и определяют перечень номеров, с которых совершаются мошеннические вызовы. Дополнительно перечень номеров, требующих уведомления со стороны оператора связи, может быть предоставлен кредитной организацией.

Кредитные организации получают в режиме реального времени (в момент вызова) по техническим каналам связи информацию о совершении звонка с номера, включенного в перечень событий.

Основываясь на полученной информации, кредитная организация по своему усмотрению принимает необходимые меры к недопущению мошеннических операций.

Использование антифрод-платформы по информированию кредитных организаций о совершении вызовов с номеров телефонов, внесенных в черный список, позволит в значительной степени снизить количество случаев мошенничества с помощью методов социальной инженерии.

4. ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ НА ФИНАНСОВОМ РЫНКЕ

Подробное описание практики

Считаем примером рекомендованной практики взаимодействие кредитных организаций и сотовых операторов в рамках прямых договоров для оперативного получения сведений, связанных с антифродовыми событиями (смена сим карты, переадресация вызова, прекращение договора абонентского обслуживания, смена пользовательского устройства и пр.).

С учетом предлагаемого в настоящее время создания единой информационной системы проверки сведений об абонентах считаем необходимым также закрепить возможность использования прямых договоров между сотовыми операторами и кредитными организациями для получения сведений по списку антифродовых событий в режиме мониторинга телефонных номеров.

Это сложившаяся практика взаимодействия банков и сотовых операторов, которую необходимо признать добросовестной. Это позволит:

1. Вывести сотовых операторов из «серой» зоны с точки зрения предоставления сведений банкам по соответствующим событиям, что позволит однозначно трактовать такое взаимодействие со стороны контрольно-надзорных органов.
2. Обеспечит банкам возможность оперативно получать сведения по номерам телефонов своих клиентов и осуществлять своевременную их защиту в случае мошеннических операций в удаленных каналах обслуживания (банковские мобильные приложения).

5. МЕХАНИЗМ ПОЛУЧЕНИЯ И ОБРАБОТКИ ОБРАЩЕНИЙ ЛИЦ, ОТКАЗАВШИХСЯ ОТ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ И/ИЛИ ОТ ОБРАБОТКИ СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Подробное описание практики

В соответствии с законодательством Российской Федерации о рекламе продвижение товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем, допускается только при условии предварительного согласия потребителя рекламы. Таким образом потребитель на законодательном уровне ограждается от контактов с теми компаниями на которые он предварительно не соглашался.

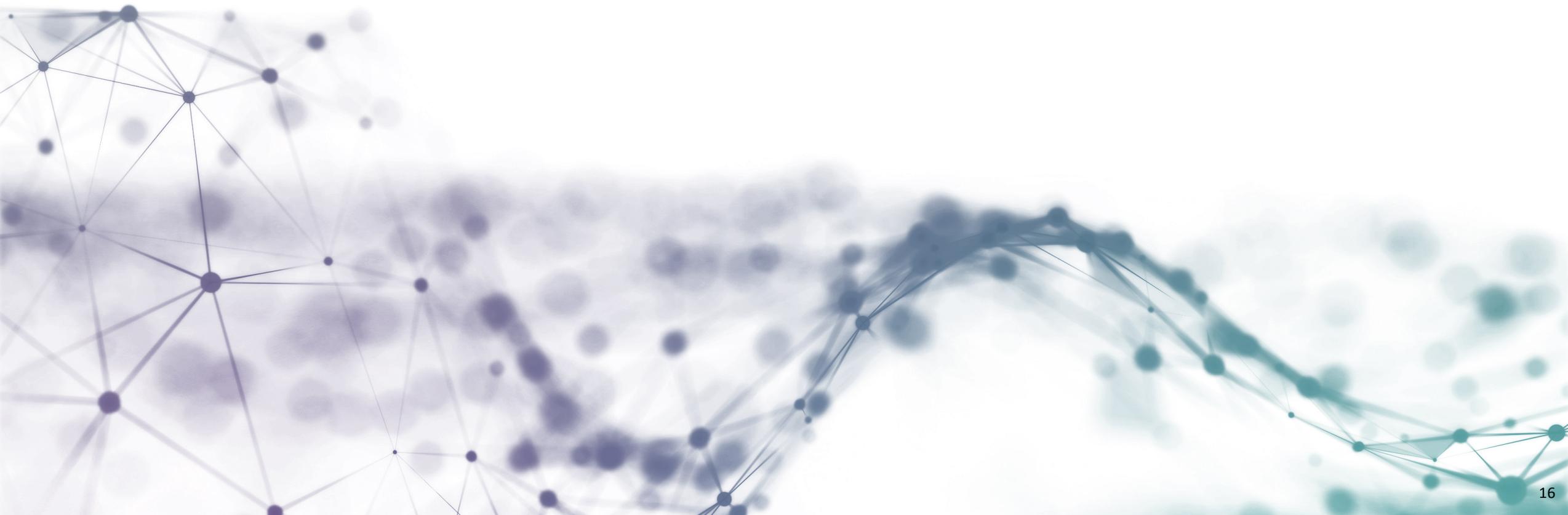
При этом, в ряде случаев, для осуществления прямых контактов с потребителем различные компании могут собирать и обрабатывать персональные данные такого потребителя. В этой ситуации потребитель может быть дополнительно защищен положениями законодательства Российской Федерации о персональных данных: так, по требованию субъекта персональных данных обработка оператором персональных данных должна быть немедленно прекращена.

В свою очередь, несмотря на наличие прямого возражения потребителя, в ряде случаев компании продолжают осуществлять прямые контакты с потребителем, что может, в зависимости от обстоятельств, приводить к нарушению законодательства о рекламе, а также законодательства о персональных данных.

Подобные ситуации возникают зачастую ввиду отсутствия у компании действенного механизма для получения и обработки требований потребителя о запрете направления ему рекламы или о прекращении обработки его персональных данных.

Считаем примером рекомендованной практики наличие у каждой компании действующего механизма получения и обработки заявлений и обращений потребителей, отказавшихся от получения рекламы или от обработки его персональных данных. В зависимости от технических и финансовых возможностей компании, такой механизм может быть реализован через соответствующее программное обеспечение, через ведение различного рода реестров (blacklists), позволяющих вести учет отказов, а также путем предоставления потребителям различных сценариев взаимодействия, упрощающих предоставление отказа (формы отказа от рассылки в самом по себе рекламном сообщении и т.п.). Наличие такого механизма у компании позволит, во-первых, сократить случаи нарушения законодательства и прав граждан, а во-вторых, будет способствовать формированию позитивного отношения к компании и ее продуктам со стороны потребителя.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ДЛЯ КЕЙСА ПО УДАЛЕННОЙ ИДЕНТИФИКАЦИИ



Банковский ID

В настоящее время есть потребность в использовании банковской идентификации с использованием банковского идентификатора гражданина (Банк ID) и предоставление сведений о нем, полученных банком в результате ранее проведенной идентификации в соответствии с ФЗ-115 (ПОД/ФТ), третьему лицу с согласия гражданина. В частности, в ряде банков существует сервис идентификации Банк ID, который может быть использован третьими лицами (компаниями) на основе коммерческих соглашений между банком и этими лицами для идентификации физических лиц, являющихся клиентами банка.

В качестве рекомендованной практики предлагаем рассмотреть в первую очередь возможность использования банковского идентификатора (Банк ID) для удаленной идентификации физических лиц в компаниях, не являющихся субъектами ФЗ-115 (ПОД/ФТ), в рамках коммерческих соглашений между компаниями и банками.

В результате такой идентификации компания, использующая сервис банковской идентификации, будет получать идентификационные сведения о физическом лице – клиенте банка (ФИО, паспортные данные, дата рождения, СНИЛС, ИНН, телефон), предоставленные банком с согласия этого клиента, выраженного банку.

В рамках реализации этой практики необходимо обеспечить актуализацию соответствующих сведений о физическом лице в банке с учетом их возможного изменения. Актуализация сведений возможна с использованием ЕСИА как государственного источника достоверных и актуальных данных о гражданине с учетом реализации концепции «цифрового профиля», предполагающей автоматическое обновление данных гражданина из соответствующих ГИСов.

В развитие – дополнительно к сервису удаленной идентификации, предоставляемой банками, может быть использована биометрическая идентификация клиента, если банк, предоставляющий такой сервис (использование Банк ID для удаленной идентификации), имеет и хранит биометрические эталоны по своим клиентам.

Мобильный ID (1 из 2)

1. Мобильный ID – сервис быстрого входа и регистрации, работающий на базе технологии SIM-пушей. Он позволяет пользователю гибко управлять собственными данными и самостоятельно определять, какую информацию предоставлять интернет-компаниям. Каждая авторизация подкрепляется разъяснениями о составе передаваемых данных и подтверждается согласием пользователя. Личный кабинет Мобильного ID при этом хранит статистику выданных согласий и состав переданных данных.

2. На наш взгляд, сервис Мобильный ID позволяет операторам персональных данных в полной мере исполнить обязанность обеспечить точность, достаточность, актуальность персональных данных следующим образом. Мобильный ID позволяет пользователям создавать цифровые профили. Пользователь может перенести свои абонентские данные в цифровой профиль, предоставив соответствующее поручение сервису. Также пользователь может давать сервису Мобильный ID поручение на предоставление данных из цифрового профиля определённому сервис-провайдеру (владельцу интернет-сайта, приложения для смартфона, видеоигры и т.д.), а в случае, если пользователь обнаруживает некорректные или неактуальные данные, он может заменить их в ручном режиме. В случае такого изменения все сервис-провайдеры, которые ранее предоставляли услуги пользователю Мобильного ID, могут быть уведомлены о таких изменениях.

3. На наш взгляд, получение подтверждения в сервисе Мобильный ID является достаточным для подтверждения получения согласия и для установления факта предоставления доступа неограниченному кругу лиц к персональным данным самим субъектом. Сервис Мобильный ID предоставляет сервис-провайдерам возможность получить авторизованное пользователем подтверждение совершения каких-либо действий в его сервисе. Для этого сервис-провайдер инициирует направление пользователю push-сообщения посредством сервиса, в момент совершения пользователем юридически значимых действий, например, выражения согласия с политикой обработки персональных данных. Информация о том, какие действия подтверждал пользователь, сохраняется у сервис-провайдера посредством log-файлов, информация о факте подтверждения пользователем своих действий или операции сохраняется сервисом Мобильный ID и передаётся сервис-провайдеру. Т.к. использование сервиса Мобильный ID неразрывно связано с услугами связи, то личность каждого пользователя ранее была установлена оператором связи в установленном законом порядке. Сервис Мобильный ID может сравнить данные, предоставленные оператору связи об абоненте-владельце номера и данные, предоставленные пользователем сервис-провайдеру при наличии согласия пользователя на обработку его персональных данных в целях такой верификации.

Мобильный ID (2 из 2)

4. Информация о соответствии (или о несоответствии) личности пользователя и реального субъекта персональных данных передаётся сервис-провайдеру и в случае необходимости может быть использована им в подтверждение правомерности обработки данных без необходимости запрашивать и получать дополнительные документы у субъекта персональных данных.

5. Технология Mobile ID как один из видов цифровых идентификаторов используется за рубежом. Цифровой идентификатор Mobile ID может применяться в следующих целях:

- упрощение процедуры совершения платежей в электронной форме (электронная коммерция), так как предполагает быстроту входа в сервис и автоматическое заполнение необходимых форм регистрации;
- подтверждение и обеспечение безопасности электронных транзакций в банках и платежных системах: вход в мобильный банк, подтверждение транзакций, анти-фрод (защита учетной записи, идентификация личности);
- обеспечение безопасности и быстрота использования ряда электронных сервисов, в частности, при покупке электронных билетов и регистрации в схемах лояльности транспортных компаний;
- взаимодействие лиц с государственными органами: вход на интернет-порталы государственных услуг, коммуникация с пользователями, обмен документами, здравоохранение и проч.

Мобильный телефон и SIM-карты также могут быть использованы при совершении авторизованных юридически значимых действий (мобильная электронная подпись).

Двухфакторная идентификация (аутентификация)

Этап 1 (Рассмотрение заявки на заключение договора)

Физическое лицо имеет возможность отправить на рассмотрение заявку на заключение договора с указанием своих паспортных данных и иной информации исключительно после предоставления соответствующих согласий:

- согласие на обработку ПД для рассмотрения его заявки;
- согласие на применение АСП (Аналога собственноручной подписи).

Согласие подписывается с помощью SMS (клиент на свой абонентский номер получает уникальный код, вводя который в форму сайта, совершает подписание согласия).

Этап 2 (Заключение кредитного договора)

Договор подписывается с помощью SMS (клиент на свой абонентский номер получает уникальный код, вводя который в форму сайта, совершает подписание согласия).

Этап 3 – Опциональный (Обмен бумажными документами)