Дмитрий Дудков (F.A.C.C.T.): Наши решения помогают банкам выполнить новые требования закона

Госдума приняла закон, согласно которому банк, допустивший перевод средств клиента на мошеннический счет, будет наказываться рублем. Дмитрий Дудков, специалист департамента Fraud Protection компании F.A.C.C.T., рассказал, как финансовым организациям подготовиться к регуляторному изменению и получить от этого максимальную пользу в борьбе с мошенниками

Фото: F.A.C.C.T.

Текст
ЕЛЕНА ПОКАТАЕВА,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

— Дмитрий, что означает принятие этого закона? Изменилась ситуация с рисками финансового мошенничества?
— Финансовое мошенничество — эта та угроза, с которой каждый день сталкиваются банки и их клиенты. Злоумышленники продолжают пробовать и использовать различные схемы для обмана и кражи денег. Количество попыток перехвата учетных записей пользователей в сервисах ДБО выросло на 59% в марте-апреле этого года по сравнению с январем-февралем 2023-го. При этом количество случаев, когда мошенник пытается подключиться через удаленный доступ к устройству жертвы, в марте-апреле увеличилось на 58% по сравнению с январем-февралем 2023 года. Количество попыток подключиться к устройствам клиентов банков в 1,7 раза превысило количество атак в целях перехвата учетных записей. Крупные банки уже давно в соответствии с требованиями 161-ФЗ используют антифрод-системы, выявляют инциденты, связанные с мошенничеством, и контролируют подозрительные переводы денежных средств. В частности, механизмы сессионного антифрода получают информацию о действиях клиента, об аномалиях, происходящих на устройстве клиента, на основании которой принимается решение, одобряющее проведение операций. Однако небольшие банки, для которых внедрение дополнительных систем защиты (антифрод-систем) слишком затратно, используют свои внутренние инструменты оценки контроля операций, не всегда эффективные.

Но помимо принудительных мер регулятор принимает дополнительные организационные меры, направленные на более эффективное противодействие мошенникам. Регулятор обязывает всех участников платежа (банк плательщика, банк получателя) проверять и приостанавливать подозрительные операции между счетами физических лиц, даже если на них имеется согласие клиента. Данные об устройствах и платежах, замеченных в мошеннических схемах, доводятся до банков.

Именно с этой целью в марте 2023 года был выпущен стандарт — единый формат сбора

данных о цифровом отпечатке устройства. Он задает перечень параметров, которые должны собираться с клиентского устройства в рамках различных каналов общения клиента с банком — через интернет или мобильные устройства.

Однако ландшафт финансовой активности клиентов банков со временем меняется, и киберпреступники активно переключаются на новые схемы. Скажем, с начала массовой релокации наших соотечественников значительно выросли объемы трансграничных переводов, а следом — и мошеннических действий. Активизировались мошенники, занимающиеся регистрацией подложных местных платежных карт.

Определенные риски появления новых схем мошенничества есть и с цифровым рублем. Ведь этот механизм позволяет человеку обращаться к своему счету цифрового рубля с любого банковского приложения в любом банке. Иными словами, после манипуляций социальной инженерии мошенник сможет распорядиться счетом цифрового рубля обманутого владельца, даже не имея при этом доступа к текущему счету. Одного лишь подхода в сборе цифрового отпечатка недостаточно, как это прописано в текущей версии законопроекта.

— Цифровые отпечатки — это новое слово в борьбе с фродом?

— Не совсем. Например, в нашей системе F.A.C.C.T. Fraud Protection используются цифровые отпечатки устройств, а также анализ «поведения» владельца устройства, выявление различных аномалий, возникающих на устройстве. Это существенно усложняет деятельность злоумышленников.

— Цифровые отпечатки, которые теперь будет собирать и Банк России, в сочетании с механизмом, реализованным в системе Fraud Protection, способны дать синергетический эффект?

— Безусловно! Мошенники ведь постоянно движутся вперед и научились подменять либо переиспользовать цифровые отпечатки. В Darknet продаются базы данных часто используемых отпечатков легитимных пользователей. И если злоумышленник начинает активно использовать эти сведения для доступа к клиентским банковским инструментам, то распыляется возможность отслеживания по цифровому отпечатку. Так что банки должны принимать дополнительные меры для анализа действий пользователя.

— У банков есть год, для того чтобы подготовиться к вступлению в силу этого закона. Им придется модернизировать свои IT-системы. Существует ли решение, которое способно решить эту задачу за финансовые организации?

— Если говорить о наших решениях, то они полноценно закрывают все потребности банков, возникающие в связи с новым законом. Помимо анализа цифрового отпечатка у нас есть запатентованная технология выявления единого идентификатора между всеми нашими клиентами. Плюс к этому используем выявление аномалий, которые происходят на стороне пользователя банковского сервиса, включая активность его действий в личном кабинете. В совокупности это позволяет практически на 100% выявлять мошеннические действия.

И это только часть функционала решения Fraud Protection. Система сессионного антифрод-менеджмента выявляет мошеннические устройства, оценивает активность пользователя во время совершения финансовых операций, выявляет автоматизированную активность (боты), что сегодня стало уже распространенной практикой. Вот почему нашими клиентами являются, по сути, все российские банки. И не только банки. Если использовать наш продукт, можно обмениваться сведениями, характеризующими мошеннические действия, как между банковскими учреждениями, так и с любыми их корпоративными клиентами, скажем торговыми организациями, страховыми компаниями и т.д. Любая компания с помощью этого инструментария сама может определить перечень данных, которыми готова поделиться, обезличить их (это важно!) и подготовить к передаче партнерам.

— В целом, как меняется со временем характер атак через ДБО?

— Мошенничество развивается волнами. Некоторое время назад наибольшая активность наблюдалась в обычных телефонных звонках, а в последние несколько лет возросла популярность звонков через мессенджеры. Это объяснимо: все время менять сим-карты — неудобно и требует усилий, да и функционал антифрода появился у операторов связи, в банковских приложениях и т.д. А в мессенджере с помощью доступных сервисов можно легко создавать множество аккаунтов и пользоваться каждым до тех пор, пока его не заблокируют по жалобам пользователей.

В настоящее время идет волна, связанная с фальсификацией указаний руководителя своим сотрудникам: в переписке в мессенджере используются данные руководителя, его фотография, сообщение от его имени, и сотрудник совершает требуемое действие, например производит платеж и т.д. И, конечно, мошенники всегда активизируются, когда появляется какая-то общественно значимая информация.

— Регуляторные барьеры в этой ситуации просто повышают порог вхождения в преступный бизнес?

— Не только. Опыт разных стран показывает, что, как только в стране начинают действовать жесткие меры по борьбе с мошенниками, поддерживаемые регулятором, и банки начинают интегрировать в свои информационные системы инструменты антифрода, мошенники переключаются на другие финансовые учреждения, где антифрод-менеджмент еще не получил широкого распространения. Фактически закручивание регуляторных гаек вытесняет мошенников на другие рынки, в том числе в другие страны.

Но противостоять финансовым мошенникам можно и на трансграничном уровне. К примеру, наше решение позволит организациям, не разглашая персональные данные, обмениваться информацией и выявлять мошеннические устройства сразу на уровне трансграничных операций. Причем мошенническая деятельность будет подтверждаться не только разметками, но и аномальной сессионной активностью. Б.О