Финансы и борьба с мошенничеством

Алексей Ананьев – технический эксперт, компания Data Integration Software.

Бурное развитие информационных технологий дало мощный толчок к появлению новых способов взаимодействия с потенциальным покупателем. Результатом этого явилось появление новых продуктов и услуг. Но, к сожалению, это явление открыло и новые возможности для разного рода мошенников. Причем, мошенники не отстают от прогресса, они также "идут в ногу со временем", осваивая технологии, изучая новые услуги и разрабатывая новые способы заработка денег на доверии людей.

Финансовые организации наиболее часто сталкиваются с различными попытками мошеннических сценариев. И, находясь в таких условиях, просто обязаны реагировать, и, более того, предупреждать подобные деяния.

Существует общепринятая методология классификации финансовых преступлений: мошенничество, легализация доходов и финансирование терроризма, также биржевое манипулирование и использование финансовой информации. В первом случае, мошенники начинают тотальную слежку за клиентом финансовой организации. Если клиент – юридическое лицо, то изучаются его способы взаимодействия с банком, перехватываются пароли входа в ДБО, проводятся попытки получить информацию через контакт-центры и т.д. Иногда один из таких путей оказывается удачным и мошенники получают доступ к банковским счетам клиента. Если мы говорим о легализации денежных средств, то здесь реализуются сценарии, в которых мошенники пытаются запутать следы и спрятать уже украденные денежные средства. Это могут быть попытки переводов денег из одного банка в другой, разделение большой суммы на много маленьких и попытка разнести их в разные банки, а потом собрать на одном счете и многое другое. Таких сценариев множество. Но, в любом случае, борьба с этим явлением сложна и крайне трудоемка. Для сценариев с манипулированием свойственны следующие сценарии: сама организация эмулирует активность вокруг своих же акций, что приводит к скачкообразному росту котировок; желание одного из менеджеров организации заработать на акциях своей компании: зная заранее о событиях, которые произойдут внутри нее в недалеком будущем и окажут влияние на повышение котировок ее акций.

Сталкиваясь с необходимостью предотвращения такого рода мошенничеств, и, понимая насколько трудоемок этот путь, финансовые организации пытаются автоматизировать процессы выявления мошеннических действий и их предотвращения.

Зачастую первые шаги в этой области – это попытка пойти по пути лоскутной автоматизации, когда под каждую задачу выбирается отдельное решение. Данный подход, при своей кажущейся простоте скрывает в себе большие организационные и технические трудности. *Во-первых*, крупная организация не может сделать покупку без проведения тендера, а это не самое простое дело и, как минимум, большие временные затраты. *Во-вторых*, на каждую из выбранных систем у организации должна быть компетенция в области поддержки и сопровождения, а с увеличением их количества экспоненциально возрастают сложность и расходы.

Есть другой, альтернативный, более прагматичный подход к решению подобных комплексных задач. Это платформенный подход. В рамках этого подхода выбирается не набор продуктов, а целая платформа, объединяющая в себе весь необходимый функционал.

Нередко поймать мошенника, используя какой то один из каналов, просто невозможно. В таких случаях может помочь кросс-канальный анализ сценариев. Именно при таком подходе возможно определить атаку на клиента путем анализа попыток входа в ДБО, звонков в контактный центр и контроля за действиями по счету. Только сопоставив все эти факты, можно сделать вывод об угрозе, нависшей над клиентом. И, согласно статистике, это примерно четверть всех случаев. Также, одним из важных механизмов контроля может быть профилирование. Финансовая организация работает с клиентом. Она знает, какие операции он обычно делает, и каким способом. Скажем, если клиент обычно пользуется банкоматом, а тут вдруг он делает перевод через интернет, то это сразу вызывает подозрение. Банк сразу увидит отклонение от обычного поведения и начнет более пристально проверять такую операцию, вплоть до личного звонка клиенту для акцепта операции. Причем, для системы контроля совершенно не важно насколько пространственно распределена транзакция. Физически клиент может находиться в другой стране, например в Англии, а мошенники – иностранцы из Аргентины – будут так же легко вычислены, как и мошенники, промышляющие в стране нахождения банка, то есть, здесь, в России.

Исходя из этого, очень важно, чтобы модули, которые ставятся на разные каналы, умели взаимодействовать друг с другом. По этой причине набирать решения от нескольких поставщиков чревато тем, что объединить эти программные модули в единый комплекс будет невозможно, поскольку интеграция этих систем между собой может быть не предусмотрена. Таким образом, для того чтобы все это работало вместе – решение должно представлять собой единое целое. И только при таком подходе можно в разы сократим время на анализ текущей ситуации и получить возможность сокращения до минимума времени реакции на попытку проведения мошеннического деяния.

Естественно, для анализа большого количества транзакций и данных из разных каналов потребуется мощное оборудование. И его мощность будет напрямую зависеть от количества анализируемых каналов и объемов данных, но, в любом случае, это не суперкомпьютеры: должно быть мощное, но серийное оборудование.

Архитектурно такое решение полностью вписывается в существующий информационный ландшафт. Для реализации блокировок транзакций – это новый слой с самостоятельным "железом" и ПО, расположенный на территории финансовой организации и находяшийся в периметре ее защиты.

Если говорить о конкретных решениях, представленных сейчас на рынке, то одним из лидеров этой отрасли можно назвать решения NICE ACTIMIZE, которые полностью охватывают каждое из описанных выше типов финансовых преступлений. NICE ACTIMIZE предлагает решения по борьбе с карточным мошенничеством, мошенничеством в контакт-центре, мошенничеством в ДБО, мошенничеством сотрудников и кредитным мошенничеством. По легализации доходов NICE ACTIMIZE может предложить анализ банковских операции в целях выявления случаев, подлежащих обязательному контролю и являющихся необычными, проверку выполняемых в банке операций на соответствие черным, белым, серым спискам, которые используются в банке. Также можно комплексно оценивать риск клиентов с точки зрения вовлечения их в процессы легализации доходов. Более того, NICE ACTIMIZE может анализировать клиентскую базу на соответствие требованиям американского закона FATCA, который приобретает все большую актуальность в России. Если брать третий тип финансовых преступлений, то NICE ACTIMIZE может предложить анализ брокерских сделок, которые идут через банк, на предмет соответствия российскому и международному законодательствам в части противодействия манипулированию рынком и использованию инсайдерской информации. Здесь программное обеспечение может так же вести белые, серые и черные списки инсайдеров, категорезируя и анализируя типологию инвестиционных сделок.

Все эти задачи различным образом работают на одной платформе, обеспечивая кросс-канальное выявление сценариев, и могут располагаться на одном железе. Таким образом, как подтверждает международный и российский опыт, подход с использованием кросс-канального анализа является наиболее выигрышным для решения комплексных задач борьбы с финансовыми преступлениями.