Тема № 8 «Мошенничество на финансовых рынках»

1. Мошенничество в финансовой сфере.
2. Традиционные методы обнаружения мошенничества.
3. Предотвращение финансового мошенничества.

1. Мошенничество в финансовой сфере.

Финансовое мошенничество в современном мире представляет один из видов социальных рисков, порожденный самим обществом. Развитие и совершенствование информационных и коммуникационных технологий привело к тому, что люди больше стали общаться с помощью компьютерных технологий, социальных сетей. Это касается и финансовой сферы, где торги ценными бумагами совершаются быстродействующими компьютерами, так как коммерческие банки предоставляют банковские услуги по интернету. Появился термин интернет-банкинг. Финансовые компании также работают с клиентами через интернет, рекламируя и продавая свои финансовые услуги.

Финансовые мошенники используют методы информационного и психологического давления на участников финансовых рынков и, прежде всего, на действующих и потенциальных инвесторов, в том числе, и на домохозяйства. Особому давлению подвергаются молодые домохозяйства и домохозяйства, не владеющие основами финансовой грамотности. Финансовые мошенники действуют во всех секторах и нишах финансового рынка. Наиболее известные виды финансового мошенничества, представлены в таблице 1.

Таблица 1 - Некоторые виды финансового мошенничества

Интернет-мошенничество
Мошенничество с использованием банковских карт
Мошенничество при покупке и продаже автомобилей
Финансовые пирамиды Мошенничество на рынке недвижимости

Сферы финансового мошенничества:

- банковская (подделка платёжных документов);

- кредитно-финансовая;
- страховая (получение выплаты несанкционированным путём);
- налоговая (неуплата налогов);
- капиталовложения;
- сеть Интернет;
- банковские карты;
- мобильная связь.

Пирамиды

Это структуры, где доход формируется за счёт финансовых вложений новых членов, и получают его те, кто вступил первым. Вступившие позднее не имеют шансов получить ни дивиденды, ни возврат средств.

Признаки мошеннической пирамиды:

- финансирование за счёт увеличения числа участников;
- неизвестность организаторов;
- отсутствие производства товаров или услуг;
- обещание больших доходов;
- широкая рекламная кампания;
- простота регистрации и вступления.

Схемы с пластиковыми картами при помощи банкоматов

1. Скимминг. Это мошенничество при помощи накладок на клавиатуру банкомата для приобретения данных карты с магнитной полосы, изготовление поддельных карт и снятие средств.
2. Шимминг. Установка считывающего элемента в картридер.
3. Установка поддельных банкоматов с целью получения данных карт без выдачи финансовых средств.
4. «Ливанская петля». В картоприемник банкомата монтируется блокиратор, который задерживает карту и она вынимается мошенником.
5. Заклеивание скотчем окна выдачи денег, их удерживание и последующее получение мошенником.
6. Установка незаметных видеокамер для фиксирования ПИН-кодов.

Схемы получения cvv-кодов

CVV-код — это трех- или четырёхзначное число с тыльной стороны пластиковой карты.

- делая покупки и производя оплату онлайн, люди сами оставляют CVV- код на мошенническом сайте;
- абоненты сотовой связи говорят сведения мошеннику, выдающему себя за сотрудника банка, или отвечают на СМС якобы от банка.

Кибер мошенничество

Данная разновидность мошенничества имеет целью получение сведений для перевода финансов с чужой карты или доступа к банковскому счету через Интернет-банк.

1. Фарминг - завладение данными карты посредством перенаправления на мошеннические сайты.
2. Фишинг - заполучение паролей пользователей Интернета вследствие сообщений на e-mail или в соцсетях, убеждающих в необходимости зарегистрировать данные на фейковом веб-ресурсе.
3. Вишинг - выманивание данных по карте с помощью звонка от «сотрудника банка».
4. «Нигерийские письма» - массовая рассылка писем с предложением вложить деньги в финансовые операции под большие проценты.

Обман при расчетно-кассовом обслуживании

1. Вытаскивание купюр из пачек, когда клиент не имеет времени посчитать их.
2. Подмена истинной валюты поддельной, а также подкладывание в пачку старых и испорченных купюр.
3. Списание с карты клиента финансовой суммы большей, чем в чеке.

Самые известные схемы телефонного мошенничества:

СМС с просьбой о финансовой помощи от родственников, якобы попавших в беду.

Уведомления о крупных выигрышах, для получения которых нужно внести плату.

Звонок от незнакомца, который якобы положил деньги на ваш номер и просит их вернуть.

Предложения от мошенников под видом сотрудников оператора связи подключить услуги посредством кодовых комбинаций.

2. Традиционные методы обнаружения мошенничества.

Общепринятые методы обнаружения и предотвращения мошенничества основаны на проведении индивидуальных расследований с возможным применением компьютерных технологий, а также на обучении и поддержке клиентов.

Простые программные подходы Компьютерные технологии могут облегчить обнаружение мошенничества, используя такие простые программные методы, как подготовка отчетов об исключительных ситуациях. В таких отчетах события, удовлетворяющие тем или иным заранее определенным критериям, получат специальную пометку. Так, например, в отчете об исключительных ситуациях при страховании здоровья могут быть помечены все операции по удалению миндалин, стоимость которых превышает определенный, заранее установленный уровень.

Такие системы используются со вполне очевидной целью — избежать крупных расходов, обращая внимание на случаи, по которым могут быть взысканы наиболее крупные суммы. Несовершенство этого метода состоит в том, что мошенники могут узнать используемые пороговые значения и не превышать их в своих сфальсифицированных документах. При этом мошенничество так и не будет раскрыто. Более сложный мониторинг может предполагать использование дополнительных пороговых значений, таких как

ставки страхования, а также другие показатели, специально разработанные для выявления мошеннической деятельности.

Обучение и поддержка покупателей и клиентов — это еще один важный компонент традиционного подхода к выявлению мошенничества. Например, можно существенно повысить надежность страхования в области здравоохранении, если направлять получателю денег подробный отчет от медицинского учреждения, предоставляющего медицинские услуги.

Это оказывается достаточно эффективным в случаях, когда мошенники используют чужие номера счетов или украденные карточки медицинского страхования. Недостатки этого метода связаны с тем, что отчеты о медицинских услугах могут содержать непреднамеренные ошибки, кроме того, в сфальсифицированных заявках могут указываться услуги, не внесенные в отчет, к тому же и сам получатель денег может не понимать или не помнить о том, какие конкретно медицинские услуги ему оказывались, или целенаправленно скрывать эту информацию.

Для успешного обнаружения мошенничества нужны оба вышеприведенных подхода; тогда их сильные стороны окажутся еще более эффективными, а недостатки будут нивелироваться. Несмотря на то, что отчет об исключительных ситуациях не несет в себе знания о том, что действительно произошло, он выдает последовательную и не предвзятую информацию. С другой стороны, именно последовательность и непредвзятость анализа прежде всего подвергается сомнению, если он проводится людьми. Правда, в этом случае можно полагаться на пациентов, которые нередко вспоминают, что происходило в действительности, и предоставляют необходимую дополнительную информацию. Недостаток обоих подходов состоит в том, что существует множество случаев, которые с трудом поддаются автоматизации, и большая часть аналитической работы в действительности выполняется людьми, а это занимает нередко месяцы, а то и годы. Улучшенные средства компьютерного мониторинга ускоряют процесс расследования подозрительных заявок, причем не просто указывают на показатели, не

соответствующие норме, но идентифицируют случаи мошенничества, а также предоставляют надежный прогноз на будущее.

Традиционные подходы к обнаружению и предотвращению мошенничества можно усовершенствовать, если ввести подготовку отчетов в число стандартных бизнес- процедур. Строгое соблюдение требований по подготовке отчетности для внутреннего персонала, а также для внешней аудитории, например, правительственных агентств, способно во многих случаях остановить мошенников, а также упростить выявление мошенничества. Хорошим примером в данном случае могут послужить требования к отчетности, оформленные недавно в США в законодательном порядке.

Для предотвращения «отмывания» денег закон о банковской тайне предписывает соответствующим банкам, а также другим финансовым организациям подавать в Министерство финансов Отчет о валютных транзакциях (Currency Transaction Report, CTR), если объем бизнес-транзакции в произвольный банковский день превысил сумму в 10 тыс. долл.

В этом отчете содержится подробная информация о личности клиента и форме оплаты, а также о финансовых учреждениях, вовлеченных в данную транзакцию. Кроме того, банкам вменяется в обязанность подавать отчет о переводе за рубеж валюты или других кредитно-денежных средств (Report of Intenational Transportation of Cuirencyor Monetary Instrument, CMIR), содержащий развернутую аналогичную информацию обо всех транзакциях с иностранными счетами (General Accounting Office 1994). Для частичного возврата ежегодных потерь в сумме 23 млрд. долл, от выплат по сфальсифицированным или ошибочным заявкам по медицинскому страхованию, Управление финансирования здравоохранения (Health Care Financing Administration, HCFA) и Американская медицинская ассоциация (American Medical Association, AMA) издали правила, согласно которым практикующие врачи обязаны предоставлять подробные истории болезни пациентов, сведения о методах обследования и процедурах, о принятых

решениях, проведенных консультациях, согласовании методов лечения, диагностике.

Вся предоставляемая информация должна сопровождаться указанием дат и сроков проведения тех или иных операций, и их продолжительности (Elliott 1998). Для пресечения воровства в страховании, Бюро страховых услуг (Insurance Services Office, Inc., ISO) объединяет данные по страхованию транспортных средств, находящиеся в распоряжении Национального бюро страховых расследований (National Insurance Crime Bureau, NICB), с базой данных заявок на выплату страховок, которую поддерживает Группа страхового обслуживания США(American Insurance Services Group, AISG) с целью формирования единой базы данных, содержащей сведения обо всех телесных повреждениях, порче собственности, компенсации служащим и заявкам, связанным с транспортными средствами (ISO 1999).

Требования к подаче отчетов обычно не могут предотвратить мошенничество; «отмывание» денег по-прежнему остается столь же распространенным видом преступной деятельности, каким оно было до выхода нового закона. Однако это может послужить для преступников предупреждением, уменьшить число случаев мошенничества, а также дать полезную информацию для правоохранительных органов об уже совершившихся преступлениях.

Помимо непосредственного выявления преступников, данные отчетов могут дать основание подозревать мошенничество. В случае с «отмыванием» денег такими индикаторами могут стать сведения о профиле компаний, вовлеченных в подозрительную транзакцию, их местоположение, частота и время совершения операций с валютой.

Дополнение традиционных методов определения мошенничества требованием обязательной отчетности повышает надежность определения случаев мошенничества, так как данные оказываются уже собранными и подготовленными для расследования. Однако расследования все еще остаются

в недостаточной степени автоматизированными и требуют проведения анализа записей непосредственно человеком.

Обнаружение мошенничества при помощи средств добычи данных Методы, предполагающие применение средств добычи данных, разительно отличаются от традиционных подходов к обнаружению мошенничества тем, что выходят далеко за рамки простых отчетов об исключительных ситуациях. Эти средства выявляют подозрительные случаи на основе шаблонов данных, позволяющих сделать предположение о мошенничестве. Шаблоны данных, указывающие на возможность мошенничества, могут обладать одной или несколькими следующими характеристиками: Необычные величины данных, каким-либо образом отличающиеся от нормы. Необычные взаимозависимости между величинами данных или записей. Изменения в поведении сторон, участвующих в транзакции.

3. Предотвращение финансового мошенничества

Предотвращение финансового мошенничества (Anti-Fraud) является насущной проблемой для финансовых учреждений. Мошенничество в российских банках колоссально увеличилось в своих масштабах за последние несколько лет. Финансовое мошенничество многообразно, а суммарный объём его в российских банках составляет миллиарды и триллионы рублей. В то же время, получение денег путём банковского мошенничества не является задачей, требующей высокой технической квалификации.

Финансовые мошенники ежедневно изменяют тактику и разрабатывают новые стратегии. Удаленные системы обнаружения признаков финансового мошенничества являются неэффективными и дорогостоящими, и они улавливают случаи мошенничества гораздо реже, чем благодаря использованию комплексных решений (так называемых, антифрод-систем).

Для предотвращения убытков, ненамеренного уклонения от ответственности перед регуляторами и защиты своей компании необходима

комплексная платформа для предотвращения мошенничества (антифрод) на уровне всего предприятия. На данный момент наиболее распространены в РФ финансовое мошенничество в каналах дистанционного обслуживания, карточное, кредитное и внутрибанковское мошенничество сотрудниками.

Для противодействия мошенничеству многие банки создают выделенные антифрод отделы и наделяют непрофильных сотрудников данными функциями, что в любом случае ведёт за собой повышение операционных расходов.

Компания DISGroup занимается одним из способов противодействия банковскому мошенничеству - системами Anti-Fraud. Данные решения совместно с другими техническими средствами позволяют эффективно выявлять такие распространённые схемы финансового мошенничества в РФ как: перехват счёта (хищение ЭЦП, подмена платежа и т.п.), фишинг, скимминг, неправомерное использование прав доступа сотрудниками Банка и т.п.

В качестве технологической платформы DISGroup применяет решения поставщика NICEActimize - признанного мирового лидера в области автоматизированных средств для противодействия различным видам финансовых преступлений. В портфель решений входят специализированные системы для противодействия финансовому мошенничеству в каналах дистанционного обслуживания юридических лиц и физических лиц, в платёжных системах, с картами, мошенничество сотрудников кредитных учреждений и др. Anti-Fraud решения применяют многоэтапный анализ и механизмы обнаружения скрытых связей для автоматизации обнаружения мошенничества и идентификации транзакций клиентов с высокой степенью риска. Решения, нацеленные на предотвращение мошенничества, содержат как готовые аналитические модели, собранные и регулярно обновляемые в результате работы со многими ведущими мировыми банками, так и позволяют реализовывать специфические правила самим пользователям системы через web-интерфейс. Алгоритмы нечеткой логики позволяют выявлять скрытые

связи между плательщиками и получателями, включая получателей с различными вариантами написания имени, получателей, использующих один и тот же филиал банка, и т.д.