

Антифрод в розничном банкинге



Практический семинар

Афанасьев Сергей

План семинара

Часть 1 Организация антифрода

- Организация антифрода
- Генезис мошенничества
- Формула мошенничества

Часть 2 Кейсы и аналитика

- Мошеннические кейсы
- Транзакционный антифрод

Часть 3 ИИ в антифроде

- Предиктивная фрод-аналитика
- Нейронные сети в антифроде
- Уязвимости нейронных сетей



10:00	Начинаем
11:40-12:00	Кофе-брейк
13:30-14:20	Обед
15:50-16:10	Кофе-брейк
18:00	Заканчиваем



Вопросы приветствуются!

Задание 1

Приведите примеры антифрод-мероприятий по типу контроля, используемых в нашем Банке

Директивные:

Детективные:

Превентивные:

Задание 2

Приведите примеры антифрод-мероприятий, используемых в нашем Банке на разных уровнях

Front (Офисы продаж, Агенты, Теле-маркетинг):

Middle (Андеррайтинг, Бэк-офис):

Back (ДББ, Риски):

БИЗНЕС-КЕЙС 1



Карточная афера

Несколько лет назад в одном крупном розничном банке запустили новый продукт под названием «Виртуальная карта». По технологии продукта, клиенту на мобильный телефон приходило SMS-сообщение с паролем и реквизитами счета по одобренному кредиту. Чтобы получить наличные, клиенту необходимо было ввести пароль и реквизиты в банкомате, то есть никаких пластиковых карт или походов в кассу не требовалось – только данные SMS.

Продукт набирал свою популярность, и с каждым днем всё больше кредитных заявок оформлялось по технологии «Виртуальная карта». Одна из таких заявок попала на проверку в подразделение андеррайтинга. Сотрудник, проверяющий заявку, выявил, что на прикрепленной к заявке фотографии изображен не клиент, а какой-то графический персонаж. Этим персонажем оказался герой компьютерной игры Tom Clancy's Splinter Cell – Сэм Фишер.



Выявленный факт был направлен на расследование в службу безопасности банка. Выяснилось, что заявка была оформлена на клиента, который уже брал кредит в банке. Сам клиент утверждал, что новую заявку он не оформлял. Также выяснилось, что перед оформлением заявки по клиенту был изменен мобильный телефон в системе банка. В процессе расследования было выявлено еще несколько заявок, оформленных на клиентов, по которым были изменены номера мобильных телефонов. Сотрудникам, проводившим расследование, стало понятно, что банк имеет дело с организованным внутренним мошенничеством.

Первой под подозрение попала сотрудница, под логином которой были оформлены мошеннические кредиты. По результатам проверки сотрудники СБ выяснили, что подозреваемая сотрудница не причастна к оформлению этих кредитов, а ее логином и паролем мог воспользоваться кто-то из недобросовестных коллег (среди сотрудников офисов негласно практиковалась передача логинов и паролей друг другу).

Круг подозреваемых расширился, было проверено и допрошено несколько действующих сотрудников офиса, включая их руководителя. По результатам проведенных проверок, была установлена личность первого мошенника. Им оказался действующий сотрудник банка Шарапов. В день оформления мошеннических кредитов он брал незапланированный отгул. Анализ лог-файлов показал, что IP-адрес, с которого оформлялись мошеннические кредиты, не принадлежал банку и использовался ранее Шараповым.

На допросе Шарапов раскрыл все детали мошеннической схемы и двух своих соучастников. Одним из соучастников оказался друг Шарапова, бывший сотрудник банка – Першин. Вторым соучастником Шарапова был Ефремов – студент московского технического ВУЗа. Мошенническая схема была следующей: Шарапов и соучастники меняли через фронт-систему банка номера мобильных телефонов клиентов на свои (дели это удаленно через «тонкий клиент» – вход через веб-браузер). После этого Ефремов приходил в банковский офис, представлялся сотрудником техподдержки банка, заходил с рабочей станции банка в программу для оформления X-Sell кредитов («толстый клиент») и оформлял заявки на этих клиентов по технологии «Виртуальная карта» (для входа в системы банка мошенники использовали логины/пароли, украденные ранее у своих коллег). В результате, на мобильные телефоны мошенников приходили SMS-сообщения со всеми данными по оформленным X-Sell кредитам. Затем вся группа ехала по банкоматам снимать наличные.

За 3 дня Шарапов и компания успели вывести около 3 млн руб., после чего их выдал Сэм Фишер – главный герой любимой компьютерной игры Першина.

На этом история с «виртуальными картами» не закончилась. Сотрудниками подразделений рисков и безопасности было выявлено еще 2 эпизода внутреннего мошенничества, где сотрудники действовали по такой же схеме, но в одиночку. Технологию «виртуальной карты» временно закрыли, банк вернул украденные деньги, а мошенники, к их счастью, остались на свободе, возместив весь ущерб, причиненный банку в результате мошеннических действий.

Задание

Напишите список мероприятий для минимизации рисков внутреннего мошенничества с "виртуальными картами".

Используйте различные методы типизации фрод-мероприятий: по типу контроля, по уровням защиты, антифрод-карту и др.

This image shows a full page of blank white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page, providing a guide for writing. There are no margins, text, or other markings on the paper.

Вспомогательные материалы




Инструменты по типу контроля:

Директивные	Детективные	Превентивные
<ul style="list-style-type: none"> - инструкции для сотрудников - договор (для клиентов и партнеров) - информационные рассылки - объявления в офисах и т.п. 	<ul style="list-style-type: none"> - антифрод-системы - системы видеонаблюдения - андеррайтинг - последующий контроль - аудиторские проверки и др. 	<ul style="list-style-type: none"> - логины/пароли - биометрия - ограничение доступов - дополнительный контроль и пр.

Инструменты по линиям защиты:

Front	Middle	Back
<p>Банковские офисы:</p> <ul style="list-style-type: none"> - проверка документов - визуальная оценка клиента - фотографирование клиента и др. <p>Сайт:</p> <ul style="list-style-type: none"> - автоматическая проверка данных - многофакторная авторизация и пр. 	<p>Верификация/андеррайтинг:</p> <ul style="list-style-type: none"> - аутентификация клиента - дополнительные вопросы - проверка клиентских данных и т.п. <p>Бэк-офис</p> <ul style="list-style-type: none"> - проверка досье 	<p>Служба безопасности:</p> <ul style="list-style-type: none"> - системы видеонаблюдения - работа с антифрод-системами - проведение расследований и др. <p>Риски/Аудит:</p> <ul style="list-style-type: none"> - анализ фрод-концентраций - разработка фрод-правил и антифрод-систем - ревизии и проверки и т.п.

Антифрод-карта

Бизнес-процессы	Аналитика	Антифрод-системы
<p> Персонал</p> <ul style="list-style-type: none"> Проверка сотрудников Обучение Организация процессов Мотивационная схема Мониторинг деятельности 	<p> Репорты</p> <ul style="list-style-type: none"> Fraud Report Concentration Report Block Report 	<p> Внутренние системы</p> <ul style="list-style-type: none"> Warning System AFS (local) и др. Black-lists Биометрия
<p> Клиенты</p> <ul style="list-style-type: none"> Идентификация клиента Визуальная оценка Андеррайтинг 	<p> Анализ портфеля</p> <ul style="list-style-type: none"> Анализ fraud-сегментов Исследования (FTI) Ad hoc 	<p> Внешние сервисы</p> <ul style="list-style-type: none"> FPS, AFS (межбанк) FPS.Bio Телеком (Мегафон и др.) Соцсети (Mail.ru и др.) Cookie (Rambler и др.) СПАРК, Контур.Фокус и др. Банкроты (Interfax)
<p> Партнеры</p> <ul style="list-style-type: none"> Партнерский договор Проверка партнеров Мониторинг деятельности 	<p> Модели</p> <ul style="list-style-type: none"> Предиктивная аналитика Разработка правил Machine Learning 	<p> Гос. сервисы</p> <ul style="list-style-type: none"> ФМС ФССП ПФР ФНС
<p> Процессы</p> <ul style="list-style-type: none"> Аудит процессов Согласование инициатив Автоматизация процессов 	<p> Оценка</p> <ul style="list-style-type: none"> СВА антифрод-процессов СВА антифрод-систем Оценка fraud-потерь 	

Задание 3

Какие антифрод-мероприятия необходимы, чтобы снизить мотивацию, возможность и обоснование?

Мотивация:

Возможность:

Обоснование:

БИЗНЕС-КЕЙС 2



Мошенничество в ФК "Открытие"

В феврале 2011 в лондонский офис ФК "Открытие" вышла команда трейдеров во главе с Джоржем Урумовым. Приобрести "талантливую" команду руководству "Открытия" настоятельно рекомендовали два сотрудника компании — начальник отдела торговли долговыми инструментами Сергей Кондратюк и трейдер Руслан Пинаев.

При переходе Урумов и его команда получили от ФК «Открытие» гарантированный бонус, который составил \$25 млн. Из полученного "гаранта" Урумов выделил \$4,75 млн четверым членам своей команды, а остальные \$20,25 млн разделил на троих с Кондратюком и Пинаевым.

Чтобы продемонстрировать свой профессионализм, команда Урумова в первый же месяц работы заключила прибыльную сделку, заработав \$2,45 млн. Позже выяснилось, что сделка была мошеннической «приманкой» и финансировалась за счет личных средств Урумова.

Согласно условиям сделки ФК "Открытие" купила аргентинские варранты (ценные бумаги, доходность которых привязана к росту ВВП Аргентины) по \$13,02 за 100 штук, а продала их по \$15,47 за 100 штук. На самом же деле варранты были куплены по рыночной цене 13 *аргентинских песо* за сотню, т.е. в 4 раза дешевле. Убыток был покрыт за счет "подъемных" средств Кондратюка, Пинаева и Урумова.

Создав прецедент, Урумов, Кондратюк и Пинаев начали готовить настоящую мошенническую сделку — покупку аргентинских варрантов у британской компании Threadneedle, в которой работал человек Урумова.

Согласно внутренним процедурам, глава риск-менеджмента инвестиционного бизнеса «Открытия» запросил реквизиты клиента и международный идентификационный код варрантов. Урумов отказался дать эту информацию, ссылаясь на то, что это требования клиента.

В марте 2011 года ФК "Открытие" оформила сделку, заплатив за варранты \$213 млн. Сделка выглядела выгодной, поскольку дисконт по рынку составил 20%. Кроме того предполагалось, что у "Открытия" есть 6-месячный форвардный контракт на продажу купленных бумаг по стоимости, обеспечивающей годовую доходность в 14%. На самом же деле варранты были куплены по цене в 3,5 раза выше рыночной.

В результате мошеннической сделки, Урумов, Пинаев и Кондратюк получили прибыль в размере \$150 млн.

В сентябре истек срок форвардного контракта, поэтому в августе Урумов с Пинаевым решили, что настало время покинуть "Открытие". Сначала Урумов, "уволит" Пинаева. А позже сам написал по электронной почте о своем увольнении и перестал отвечать на звонки и sms.

В конце августа в "Открытии" узнали настоящую стоимость варрантов. Началось расследование. Выяснилось, что одна из сотрудниц мидл-офиса знала про завышенную стоимость бумаг и рассылала письмо по отделу о том, что сделка прошла по курсу аргентинского песо 1:1 вместо 4:1. Бэк-офис и подразделение рисков регулярно задавали вопросы по стоимости варрантов. Но поскольку в мошенническую схему было вовлечено несколько сотрудников разного уровня, коммуникация возвращалась к кому-то из участников аферы, которые подтверждали, что все в порядке.

В результате розыскных мероприятий Урумов и Кондратюк были задержаны и арестованы, Пинаеву удалось скрыться в Израиле. В Британии и Швейцарии на них были заведены уголовные дела.

"Открытие" по решению суда начала замораживать активы мошенников и возвращать украденные средства. Суд постановил, что ответчики должны возместить в общей сложности \$200 млн, с учетом процентов и судебных издержек.

Задание

1. Перечислите – какие процедуры контроля при проведении сделок были нарушены в компании?

[illegible]

2. Какие антифрод-мероприятия необходимо реализовать, чтобы минимизировать риски подобного рода внутреннего мошенничества в будущем?

This image shows a single sheet of white paper with horizontal blue ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

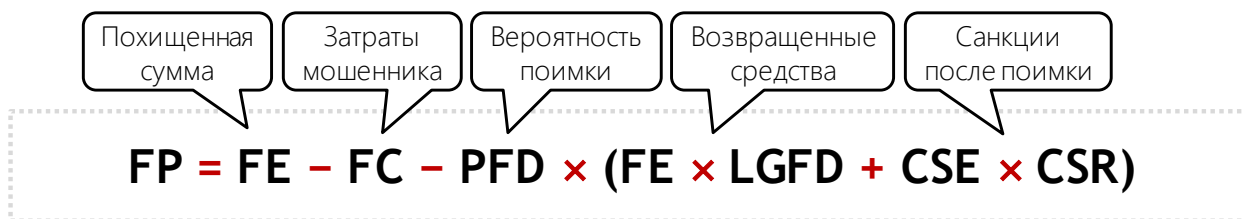
3. Какие антифрод-мероприятия необходимо реализовать в компании, чтобы данный тип мошенничества стал невыгодным для сотрудников? Заполните таблицу.

Переменная	Влияние на переменную	Антифрод-мероприятия
FC Стоимость затрат мошенника	Повысить	
FE Похищенные мошенником средства	Снизить	
PFD Вероятность раскрытия мошенничества	Повысить	
LGFD Доля возвращенных средств	Повысить	
CSE Потери вследствие понесенного наказания	Повысить	
CSR Доля смягчения наказания.	Снизить	

4*. Оцените фрод-профит (FP) по формуле мошенничества, подставляя в формулу свои экспертные значения переменных.

Вспомогательные материалы

Формула мошенничества:


$$FP = FE - FC - PFD \times (FE \times LGFD + CSE \times CSR)$$

Прибыль от мошенничества (*Fraud Profit – FP*) – прибыль, которую ожидает получить мошенник, учитывая свои риски и издержки;

Подверженность риску мошенничества (*Fraud Exposure – FE*) – экономическая оценка похищенных мошенниками активов;

Стоимость трудозатрат мошенника (*Fraud Costs – FC*) – складывается из стоимости потраченного времени, вложенных инвестиций и других расходов мошенника;

Вероятность раскрытия мошенничества (*Probability Fraud Detection – PFD*) – оценивается путем статистического анализа раскрытых и нераскрытых мошеннических фактов;

Уровень возвращенных средств (*Loss Given Fraud Detection – LGFD*) – доля возвращенных средств, в случае раскрытия мошенничества;

Подверженность уголовному наказанию (*Criminal Sanction Exposure – CSE*) – стоимость максимальных личных потерь мошенника вследствие уголовного наказания (штраф, потеря оплачиваемой работы на период отбывания наказания, потеря репутации и т. д.);

Степень жесткости наказания (*Criminal Sanction Ratio – CSR*) – уровень личных потерь, понесенных вследствие смягчения наказания (штраф вместо уголовного наказания, условный или неполный срок и т.д.).

БИЗНЕС-КЕЙС 3



Мошенничество на \$3.000.000

В 2012 году одним крупным розничным банком произошел довольно интересный случай внутреннего мошенничества. Группа сотрудников Уфимского банковского офиса в составе руководителя группы продаж и трех его подчиненных оформляли мошеннические кредиты по поддельным документам. Мошенническая схема была достаточно распространенной и хорошо известной аналитикам и сотрудникам безопасности банка. Уникальность ситуации заключалась в том, что мошенники в течение 4-х месяцев оформляли мошеннические кредиты, а финальные потери оказались самыми большими за 10-летнюю историю работы банка на рынке розничного кредитования.

Первые попытки оформления мошеннических кредитов начались в октябре. Через несколько дней антифрод-система выдала первый сигнал. Аналитик обработал кейс и направил его на расследование сотруднику безопасности. Несколько выявленных фактов указывали на мошеннические действия со стороны сотрудников банка:

- 1) Кредиты оформляли по украденным паспортам (по данным сервиса ФМС);
- 2) У разных заемщиков совпадали номера страховых свидетельств;
- 3) У разных заемщиков совпадали номера мобильных телефонов.

В декабре сотрудник безопасности прислал ответ: «Платежи по кредитам вносятся своевременно, просрочки нет. Мошенничество не выявлено». Аналитик решил не спорить с выводами сотрудника безопасности и ушел в отпуск на новогодние каникулы.

В январе после праздников антифрод-система повторно выдала сигнал по тем же самым сотрудникам. Факты были аналогичные: кредиты оформлялись по поддельным паспортам, по разным заемщикам указывались одинаковые номера вторых документов и одинаковые номера мобильных телефонов. К выявленным фактам добавились еще результаты звонков call-центра, согласно которым, большая часть оформленных клиентов были неконтактны. Аналитик также выявил, что первые 3 платежа по выданным кредитам вносились в течение одного часа и с одного терминала (поэтому показатели просрочки по сотрудникам были почти нулевые). Материалы повторно были направлены в службу безопасности, которая на этот раз вынесла вердикт: «внутреннее мошенничество». В феврале всех участников мошеннической схемы заблокировали. За четыре месяца своей деятельности они успели вывести из банка порядка \$3.000.000.

Стоит отметить, что за последние 5 лет работы между сотрудниками департамента Рисков (в котором работали аналитики) и Службой Безопасности сложились сложные корпоративные отношения. Взаимодействие аналитиков строилось напрямую с региональными сотрудниками СБ: аналитики выгружали информацию по кредитным заявкам, проверяли подозрительные факты и направляли кейсы напрямую в регионы. За каждым из 80 регионов присутствия банка, был закреплен отдельный сотрудник СБ. С некоторыми регионами регулярно возникали споры и конфликтные ситуации на тему корректности присылаемой на расследование информации. Поэтому очень часто отрицательное решение сотрудников службы безопасности по мошенническим кейсам не оспаривалось аналитиками.

Задание

1. Система фрод-мониторинга сработала когда потери банка составляли \$600.000. Финальные потери по этому эпизоду выросли в 5 раз и составили \$3.000.000. Опишите, какие банковские процессы были несовершенны, что привело к такому результату?

2. Как повысить качество процедур расследования, чтобы в будущем не возникало таких ситуаций?

Задание 4

Приведите примеры схем транзакционного мошенничества с картами и интернет-платежами

[illegible]

Задание 5

Напишите типы нейронных сетей и виды обучения в Machine Learning

Нейронные сети:

Виды обучения в ML:

Задание 6

Перечислите виды биометрических систем, которые используются в нашем Банке и которые не используются (какие знаете)

Используются в Банке:

Не используются в Банке:
