БИОМЕТРИЯ ДЛЯ ВЫЯВЛЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ ПРИ ОФОРМЛЕНИИ КРЕДИТОВ

ДЛЯ КОГО:
Службы Безопасности Банков

ПРЕДПОСЫЛКИ К ВНЕДРЕНИЮ СИСТЕМЫ БИОМЕТРИИ

Согласно оценке ведущих банков на сегодняшний день в Российской Федерации выдается мошеннических кредитов на сумму несколько десятков миллионов долларов в год – это прямые убытки Банка, которые негативно отражаются на финансовой отчетности.
Согласно наблюдениям Служб Безопасности Банков наиболее распространены 2 схемы мошенничества:

1) Получение кредита по поддельным документам
2) Получение кредита по поддельным анкетным данным

Получение кредита по поддельным документам

При данной схеме мошенники используют чужие личные данные в поддельных паспортах. Для простоты получения кредита обычно используются личные данные граждан с положительной кредитной историей. При этом в поддельном паспорте используется фотография мошенника, оформляющего кредит.
В результате таких неправомочных действий гражданин, данные которого использовались для мошеннического получения кредита, узнаёт о необходимости платить за кредит после того, как деньги мошенниками получены. В таких случаях клиентам необходимо доказывать в суде непричастность к получению кредита. В результате:

- моральный и материальный ущерб клиент (если это существующий клиент банка, то с высокой степенью вероятности он прекратит сотрудничество и перейдет на обслуживание в другой Банк)
- материальный ущерб Банка (потери в виде невыплаченного кредита, расходы на судебные тяжбы с клиентом, оплата услуг коллекторов).

Центр Речевых Технологий

САНКТ-ПЕТЕРБУРГ
(+7 812) 325-88-48
stc-spb@speechpro.com

МОСКВА
(+7 495) 669-74-40
stc-msk@speechpro.com

WWW.SPEECHPRO.RU

Существующая сегодня схема проверки заявителя базируется на проверке паспортных и указанных в анкете данных – по базам данных ”черных” списков, базам агентств кредитных историй, алгоритмах оценки кредитоспособности скоринговых систем и пр. Но все эти проверки оказываются абсолютно неэффективными, когда мошенники используют данные реального человека с положительным кредитным профилем.

РЕШЕНИЕ

Надежным решением описанной проблемы является применение автоматической фотобиометрии в процессе обработки заявления на получение кредита. Фотобиометрия – это технология распознавания или сравнения людей по лицу. В отличие от субъективного анализа лица человеком, системы фотобиометрии способны в автоматическом режиме, объективно, с высокой степенью точности определить сходство нескольких лиц между собой. Для применения фотобиометрических технологий в банке достаточно сформировать фотобиометрическую базу клиентов – на основе фотографий клиентов, получаемых при визите в банк или по фотографиям клиентов со сканированных копий паспортов.

При использовании фотобиометрической системы, сотрудник, оформляющий заявку на кредит, дополнительно к заполненной анкете должен сфотографировать заявителя. Далее при обработке заявки на кредит системами банка дополнительно к стандартным проверкам персональных данных заявителя проводится фотобиометрическая проверка фотографии заявителя.
Проверка паспортных данных проходит успешно. Но модуль биометрического учета обнаруживает, что фотографии заявителя не совпадает с фото клиента Банка, имеющегося в базе данных. В случае неуспешной фотобиометрической проверки заявителю отказывается в получении кредита, фотография заявителя заносится в «чёрные» списки мошенников.

Решение фотобиометрии от «Центра речевых технологий» позволяет:

- формировать базу клиентов Банка по существующим фотографиям
- формировать базу клиентов банка по фотографиям сканированных копий паспортов клиентов
- формировать “черные” списки мошенников
- интегрировать фотобиометрию с существующими скоринговыми системами Банка
- проводить фотобиометрическую проверку в автоматическом или ручном режиме

ЭФФЕКТ ОТ ВНЕДРЕНИЯ

Банк получает дополнительную степень защиты от мошеннических действий при оформлении и выдаче кредитов, тем самым уменьшая размер потерь от мошеннических действий.

Добросовестные клиенты Банка защищаются от неожиданных финансовых и моральных издержек.

Получение кредита по поддельным анкетным данным

На сегодняшний день кредитное мошенничество приобрело широкий размах и для оформления кредита используются фиктивные компании и поддельные справки о доходах. Данный вид мошенничества (т.н. оформление кредита “на лося”) заключается в сговоре мошенников с гражданами (обычно привлекаются люди неблагополучных слоев населения), с целью получения в банках крупных кредитных сумм. В данной схеме гражданину, согласившемуся на неправомерные действия, оформляется фиктивное место работы, выписывается справка о доходах, а в анкете-заявлении на кредит указываются телефоны подставных “бухгалтеров” и “руководителей” компаний-работодателей.

Полученный по такой схеме кредит не выплачивается и ведет к финансовым потерям банка (невыплаченный кредит, услуги коллекторов).

Существующая сегодня схема проверки заявителя базируется на проверке паспортных и указанных в анкете данных – по базам данных ”черных” списков, базам агентств кредитных историй, алгоритмах оценки кредитоспособности скоринговых систем и пр. И все эти проверки заявитель успешно проходит, т.к. по всем указанным в анкете телефонным номерам организации-работодателя с готовностью подтверждают анкетные данные “бухгалтеры” и “руководители”.

РЕШЕНИЕ

Надежным способом решения описанного способа мошенничества является применение голосовой биометрии при обзвоне по указанным в анкете номерам телефонов компании-работодателя. Проверка личности собеседника по голосу – это единственный надежный способ удаленной идентификации в условиях, когда личная встреча с клиентом невозможна.

Обычно мошенники сами отвечают на звонки, представляясь “бухгалтерами” и “руководителями” работодателя, и подтверждают все фиктивные анкетные данные. Сформировав базу данных голосов мошенников по предыдущим мошенническим случаям, с использованием системы голосовой биометрии можно проверять голос собеседника и сравнивать его с голосами мошенников, имеющимся в базе. В случае совпадения голосов, заявление на кредит должно подвергаться дополнительной проверки Службы Безопасности Банка или, в случае высокого сходства голосов, должен автоматически формироваться отказ в предоставлении кредита.

Решение «Центра речевых технологий» VoiceKey.AGENT основывается не технологиях голосовой биометрии и позволяет:

- формировать базу голосов мошенников по существующим записям контакт-центра
- автоматически сравнивать голоса собеседников с голосами мошенников
- формировать отчеты о найденных совпадениях
- осуществлять сравнение голосов как в ручном, так и в автоматическом режимах.
- загружать базу голосов мошенников из внешних источников

ЭФФЕКТ ОТ ВНЕДРЕНИЯ

Банк получает дополнительную степень защиты от мошеннических действий при оформлении и выдаче кредитов, тем самым уменьшая размер потерь от мошеннических действий.