STEPPING UP AGAINST AUTHORIZED FRAUD

Strengthening Trust in the Payments Process

CELENT

STEPPING UP AGAINST AUTHORIZED FRAUD

STRENGTHENING TRUST IN THE PAYMENTS PROCESS

Gareth Lodge
August 2020

This report was commissioned by Nice Actimize, at whose request Celent developed this research. The analysis and conclusions are Celent's alone, and Nice Actimize had no editorial control over report contents.

OLIVER WYMAN

AUTHORIZED FRAUD – WHY BANKS NEED TO CARE

WHY SHOULD BANKS CARE ABOUT AUTHORIZED FRAUD?

At face value, while many banks will feel some sympathy if their client was impacted by fraud, unless the bank was clearly responsible, the bank would ensure that they didn't cover the losses, and as rigorously as possible. After all, banks are businesses and losses can have a material impact on margins. They may *choose* to reimburse, but that will be part of their business strategy.

Banks have seen fraud rise steadily over the last few years, and so now are more active in managing their own losses, both through polices and technologies. Furthermore, new rules and regulations often focus on consumer customer protection, such as Secure Customer Authentication that actively measures and indeed, punishes banks for high levels of fraud. As a result, consumer fraud is actively pursued by the industry. Most countries don't have any clear liability framework for corporate fraud, and often don't even track such fraud. Even where there are frameworks, such as Confirmation of Payee in the UK, they are often voluntary.

If that fraud fell under the category of Authorized Fraud, the banks would feel pretty sure that they bore no responsibility at all — after all, as the saying goes, the clue is in the title! They may also feel that the fraud is out of their scope, as it is fraud taking place inside another organization. Yet that would be a narrow view, especially with corporations. In a survey in 2018, The Association for Financial Processionals (AFP), reported that 80% of surveyed businesses reported being targeted by just one specific type of Authorized Fraud attempt, Business Email Compromise. While the group may or may not be statistically representative, it is safe to say that it is extremely widespread, especially as its likely as some attempts will have also not have been reported or even detected. Given these attacks also typically result in higher value transactions, often measured in millions, that the banks execute the payment instruction for, then the stakes for the industry are quite high. Yet it is also surely an opportunity for a bank to differentiate themselves. A bank offering additional protection that could save the corporation a significant sum of money may well be a key differentiator between banks competing for their business. There is also the stark possibility that faces the banks if those businesses go insolvent as a result of the losses. The cost of fighting the root cause probably outweighs the cost of what happens as a result, especially as we enter a period of likely recession.

WHY NOW?

Before these difficult times, banks had increased the money they spent to reduce their fraud losses, albeit often because they were told to do so by a regulator. As a result of Covid-19, every central bank globally is predicting that their country is about to enter a deep recession, with some predicting that it may be many years before they recover. In the last financial crisis, bank IT spending was dramatically reduced. Many banks froze or cancelled all but the most essential IT projects, and of those projects that continued, nearly all were pared back to the bare minimum required. Banks already have a large set of regulatory projects that they have to do, such as the migration of Swift messages from MT to MX. So why should banks expand their spending to Authorized Fraud, especially from corporate clients if there is no regulatory pressure to do so?

There are a few reasons that could be considered as pre-emptive. It is likely, for example, that regulators globally will increasingly make voluntary schemes mandatory, and will look to treat customers of all types the same. This is especially true as some regulations

arguably apply already. Under anti-money laundering regulations, banks already have to check all in-bound transactions for suspicious activity. Many Authorized Fraud scams involve accounts set up specifically for the purpose of the fraud, and often with names that look like those of a real company, so as not to be noticed by the sending corporation. The receiving bank in this instance has several points of responsibility. The first is the inbound transaction. It is unlikely that the account will have previously handled many transactions, and certainly not one of the values associated with Authorized Fraud, so there should be some immediate flags. Second, during the account opening process, Know Your Customer processes should ensure that the name of the account doesn't raise suspicions.

Instant Payments and Open Banking are also potentially creating issues. Instant Payments aren't inherently more risky, but they do mean that issues are exposed that much quicker. Some instant payment schemes are actively addressing the issues. The rules for Request To Payment, run by The Clearing House, clearly state a number of obligations over and above those listed previously by the bank holding the requesting account. Open Banking may be considered risky for a similar reason — how easy is it for a corporation to check not just what permissions have been granted, but to whom or by whom? Many of the use cases involve Instant Payments, Open Banking, and automation, so it isn't too much of a stretch of the imagination to believe things designed to make life better will for the same reason, make things worse.

But there are other reasons why specifically that banks should *now* address this and many of these are Covid-19 related. It is extremely likely that there will be large upticks in all forms of fraud, including Authorized Fraud, as "normal" is displaced with processes and procedures that weren't ever designed for large scale remote working — or in some instances, ever designed. Furthermore, there are many non-standard payments and procurements taking place currently, with many new suppliers being added. It is easy then to see the situation where a fake CEO rings an account assistant to make an urgent payment, using a cloned phone number. That assistant can't ask the person sitting next to them any longer, nor will they know if the CEO is in the building like they could before.

Given how widespread business email compromises fraud already, coupled with many companies in very fragile states as a result of the recession, an uptick quickly takes on more serious implications. Losses could well mean bankruptcy for some firms, and that will have a knock-on effect as they will no longer be able to fulfill their orders or pay their suppliers. This obviously means a loss of revenue for the bank, but also additional cost as they respond to the domino effect that this might cause.

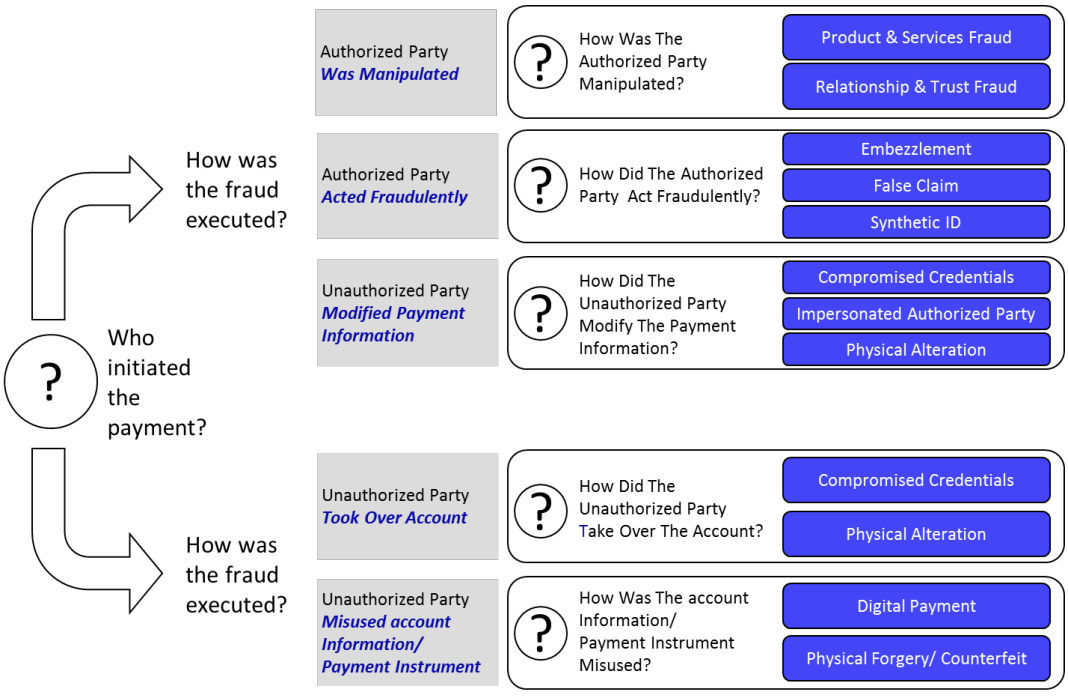
The Silver Lining?

While no-one believes that anybody should benefit from others' misfortunes, there are things that banks could do in response to these scams where they will ultimately benefit in some way. Rather than waiting for the regulator to intervene, a bank could take a leadership role and decide to use this as a point of differentiation. There are a number of ways the bank could benefit, from seeing as caring for its customers, to protecting its own interests, to reducing operational costs post fraud. Many of the actions are (relatively) low cost, at least compared to some of the risks. For example, a key activity will be educating clients, which could be bundled into a broader out-reach activity. Central to the activity will be the bank itself understanding the types of fraud in order to best ascertain its role and where it could or should intervene.

GRASPING THE ISSUE

The Federal Reserve has a Fraud Classifier Model, which is a great starting point. This can seen in Figure 1 below.

Figure 1: Federal Reserve Fraud Classifier Model



Source: Federal Reserve

At first glance, it would be easy to assume both that there were only a handful of types of Authorized Fraud, and that all Authorized Fraud was the same. Indeed, there are some aspects that are common to all types of Authorized fraud. Yet to do so would miss many important subtleties, and perhaps more importantly here, would obfuscate where banks have a role that they can play.

Key is understanding the myriad of variations. While only three types of Authorized Fraud are addressed here, just one of those (Business Email Compromise) can be broken down into at least six distinct variations just focusing on corporations! Each of these attack vectors potentially exploits weaknesses in the policies and procedures of corporations, many of which are specific to that vector, before we begin to think about the opportunities for detection. Furthermore, they overlap the other types of fraud considered here, CEO Fraud and Investment Fraud may be committed by email.

CEO Fraud is where a third party impersonates the CEO in some way, and usually to demand a more junior member of staff make an urgent, non-standard payment. That impersonation may be through spoofing the number of the CEO, to taking over their email account, or simply pretending via a personal email account ("I've had my phone stolen so having to use my personal email address."). The latter may not seem very sophisticated, but, coupled with being armed with the right information (like personal details about the recipient), can be surprisingly effective.

Equally, there are some increasingly sophisticated CEO frauds. In March 2019, a senior manager at a UK energy company was called by his German boss to urgently transfer money to a Hungarian supplier, with which he complied. A second call came the next day, from an Austrian number to say that the payment would be reimbursed from the head office shortly. It was while he was speaking to his boss that he received a third call from "his boss." and they realized that it must be a "deep fake," an artificially generated voice that was calling. The energy firm lost £243,000. What is worth highlighting is that the German boss was speaking English, and had quite an unusual accent, yet his colleague who regularly spoke to him didn't notice the difference.

The urgency is the common factor with Investment Fraud as well. Here the fraudsters try to create a "Fear of Missing Out" by offering a time limited opportunity to invest at a discounted price and ask for money in advance. This may be an investment, but as often to buy supplies, neither of which materialize despite the advance payment.

While the other types of fraud are important, it is worth highlighting Business Email Compromise (BEC) fraud specifically because of the sheer scale of the issue, both prevalence as well as losses. CEO Fraud, and deep fake attempts are relatively rare, but BEC fraud is by far the most common. It is very cheap for the fraudsters to orchestrate, and can be run at scale, making the potential of success that much greater.

What is Business Email Compromise?

The FBI's Internet Crime Complaint Centre (IC3) defines Business Email Compromise (BEC) as:

> *Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds request.*
>
> *The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.*
>
> *The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information or Wage and Tax Statement (W-2) forms.*

Banks have very strong security, and very active programs around phishing and social engineering, so it often comes as a shock not just how prevalent this is, but also the scale of the issue. After all, who hasn't had an email at home from a supposed online shop asking them to reenter their financial details. Yet, the scam is more than widespread, but is almost universal. In a survey in 2018, The Association for Financial Professionals (AFP), reported that 80% of surveyed businesses reported being targeted by Business Email Compromise. While the group may or may not be statistically representative, it is safe to say it's likely even higher, as some attempts will not have been reported or even detected. To put the numbers into greater perspective, the US Treasury Department believes that in 2016, 500 businesses lost money to BEC… a month. In 2019, they revised that to 1,100, with an aggregate average *monthly* loss of $300 million.

There are also many different flavors of BEC:

- BEC Business Email Compromise
- VIS Vendor Impersonation
- CEO CEO Fraud Impersonation
- PCS Payroll Compromise Scheme
- ERS Expense Report Scam
- MCS Mortgage Closing Scam

It is likely that not only will each firm have had an attempt; it's likely that they will have multiple types of attempt.

The Losses Are Potentially Significant

The IC3 reports on victims of fraud, and while they don't separate out attempted and actual fraud, the numbers are still staggering. Between October 2013 and July 2019, there were 69,384 US victim reports, with $10.1 billion targeted. It is a global phenomenon as well. Between June 2016 and July 2019, there were 166,349 victim reports that the IC3 were aware of, totaling $26.2 billion, from 177 countries.

It isn't just the number of attempts that is eye opening to banks, but the success that the fraudsters have. There are only a handful of cases that hit the headlines, but they give an indication of the scale of the issue. One of the more infamous cases is that of a Lithuanian syndicate led by Evaldas Rimasauskas. Beginning in 2013, his team regularly called the customer service centers of Facebook and Google.

Through this they gained the names of key employees and relevant contact information. They also used phishing emails to gain access to the respective email systems of the two companies and gain further data of value. Using this information, they identified the name of a supplier and created bank accounts with similar names to the supplier. After two years of working through this process, the fraudsters eventually called each company pretending to be that vendor, and had both companies change destination bank account numbers to ones that they owned. The syndicate then submitted and requested payments against fictional invoices. Facebook transferred $99 million and Google $23 million. The funds were then quickly wired on to a range of other accounts controlled by the syndicate.

This is far from an isolated incident — Nikkei, the Japanese media company, announced in October 2019 that they had lost $29 million to a similar scheme. It should be no surprise then that the FBI considers BEC to be the greatest fraud threat to businesses.

There are many aspects to the Rimasauskas fraud that are worth highlighting. First, it is often assumed that the victims are smaller, less sophisticated businesses, perhaps less internet savvy and with lower security. The victims in this particular case highlight that this is far from the case. Even the most technologically advanced businesses are at risk. Indeed, arguably bigger businesses make better targets as they both offer richer rewards but that they are also sufficiently large that abnormal requests are perhaps more normal.

Second, many banks will have assumed that the values are small, whereas the sums involved are often significant. Third, these are long-term, multi-pronged attacks. These aren't just blanket approaches, but very targeted, and relying on detailed research to make the fraud happen. Given the sums involved though, the rewards are worth the investment by the fraudster.

The Anatomy of a Fraud Attempt

The Rimasauskas case and the UK energy deep fake fraud give some idea of some of the stages of the fraud. These can broadly be grouped into three stages: research, planning, and execution.

Research is the laying of the groundwork. In the Rimasauskas case, the research was substantial, not least with targeting those two victims. Over the course of two years, using social engineering and hacking, they had to not just identify the key contacts within the two targets who could authorize the transfers, but the names of the key vendors, *and* the likely size of spending with those vendors. For example, if they had requested those sums for a vendor who was infrequently used or for low value transactions, then the requests would have been more likely to have been caught. In the deep fake case, there was substantial research, involving the identification of specific individuals, types of payment, and of course, the voice. It wasn't just the voice pattern but the language as well, showing the level of preparation that is often put in place. Given the potential returns, this shouldn't come as a surprise.

Planning is the orchestration of the fraud, organizing the required information and tools. In the Rimasauskas case, this included the creation of a registered business in Latvia that was similar to the existing supplier, before setting up a bank account in Latvia as well as two accounts as the same country as the real vendor, along with the false invoices that would trigger the payments, that matched the invoices that victims received. That likely means obtaining copies of original invoices. The planning may be the first stage, rather than following the research phase. For example, in an investment fraud, they may know what they want to sell, but they need to identify victims to sell to. There are many examples currently in the press around PPE equipment that would suggest that fraudsters may have seized upon the demand and urgency and have looked for victims to sell the fictional goods to, or shares in companies to produce such items.

The execution piece is more complex than it might first seem. In CEO fraud, the fraudsters need to know when the CEO is uncontactable, and during banking hours. This narrows the window to very specific times. It also then requires the fraudsters to act quickly once the funds are received. For example, in the Rimasauskas case, they transferred the funds as quickly as possible to banks in, among other places, Latvia, Cyprus, Slovakia, Lithuania, Hungary, and Hong Kong, before it was further dispersed from there.

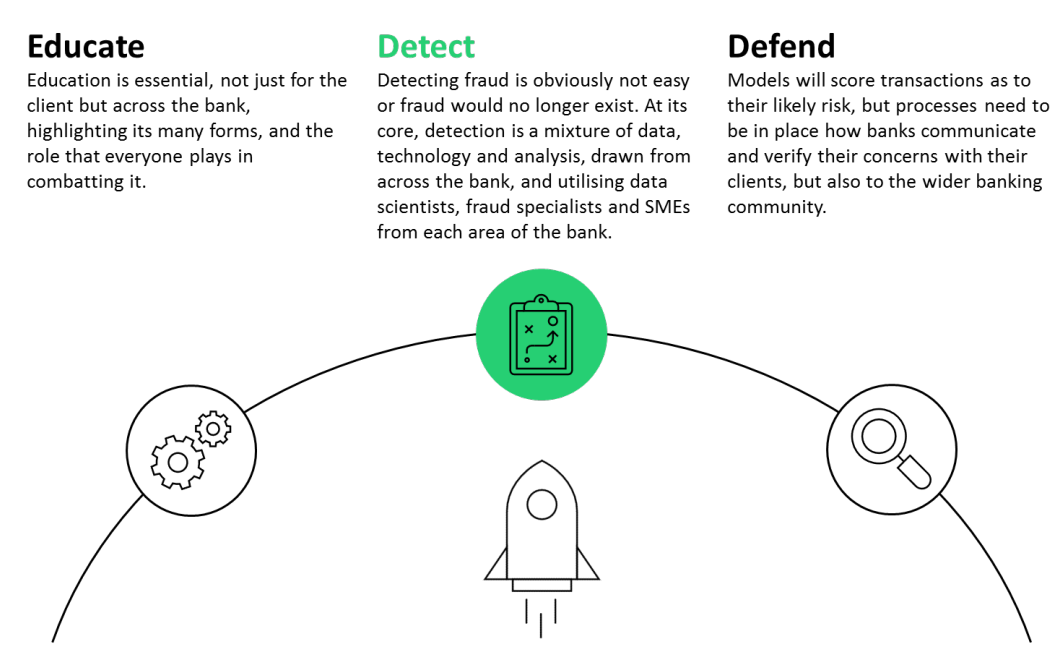
Initially, it may seem that the bank has no role to play in stopping any of these three phases. However, there are multiple points that can both disrupt but also detect activity.

ACTIONS FOR BANKS TO TAKE

Previous sections have shown clearly why banks need to pay more attention, yet for some it may not be clear about quite what they actually do. Central to their action is their unique position in the value chain, sitting at the center of any commercial transaction. As a result, they have greater visibility than almost anyone into the flows of transactions. While an ACH may process more transactions, they won't see which login initiated a transaction or know whether it looks different from others. It is often the context of the payment that is the indicator that something isn't right.

Banks can undertake three different activities to help their clients: educate, detect, and defend. These can be standalone activities, but obviously greater success will be found by not only doing all three, but coordinating between them to create a more holistic program. That may sound obvious yet often is not the case within the bank as individual activities are often owned by different people.

Figure 2: Three Core Measures Will Be Required by Banks To Tackle Authorized Fraud



Source: Celent

EDUCATE, EDUCATE, EDUCATE

At the heart of any activity should be education, not just of the banks' corporate clients, but across the bank as well. Authorized Fraud isn't just the Fraud departments concern, but anyone in contact with the client. Given some of the mechanics of Authorized Fraud, such as the need to set up a new payable account, it is as likely that another part of the team will catch the fraud attempt.

Here defining the types of fraud in greater granularity will aid detection. While many of us in our home life will recognize some of the cruder, more widespread activities that take place, like phishing, highlighting not just how sophisticated the fraud is but how others who have fallen victim will press home the need for close attention. The different types of fraud allow the bank to reach out regularly to the client, particularly as Relationship Managers are always looking for more touchpoints.

It isn't just enough to tell clients about what to look for, but how to prepare as well, particularly in terms of best practice, and agreeing processes. For example, if a corporation wants to change the account details for an existing supplier, how should the corporation go about it? Do all changes have to be done by specific, named people? Should the RM validate the request with a different named individual?

DETECT

Detecting fraud is obviously not easy or fraud would no longer exist. At its core, detection is a mixture of data, technology, and analysis. Strengthening any of these will improve the results; conversely, a weakness in any of them will limit the success of the results. They're increasingly interlinked — the analysis is done by the technology, and the technology will do much of the necessary normalization of data. Yet it is still worth considering them separately.

Data

The challenge with data for a bank is not the lack of it. After all, banks collect data from the clients daily, via every interaction the client has with the bank. Instead the challenge is two-fold. First, the first challenge is the sheer volume of data that is available. Every product, every channel in every part of the bank is generating and storing data, usually in isolation. Take a "simple" transaction. The entitlements engine defines who can make a transaction, and what they can do. The channel will log data appropriate to its usage, from IP addresses to customer journey. The current balances are stored in the general ledger. The controls over what a specific account can do, such as limits, are stored in the Customer Information File. The nominated account details are stored in the payment engine, which will be specific to the payment type. If done, the checks on the account will be taken from AML and OFAC engines. And the resulting transaction is stored in a payments database, usually stored by payment type. And this is just the simplistic view!

Furthermore, none of the data stores are storing data in the same way. This isn't just how it is stored (as in the underlying database), but also what is stored. Given that they are usually by-products of different processes, often there isn't even a common identifier to link these data elements across processes, but just usually within that specific process, and may be either structured or unstructured.

Second then is the identification of the *right* data, which is often spread across many disparate databases across the bank. Data lakes and data stores have been attempted by many banks, but few perhaps have been truly successful. It is likely then that the bank will need to identify all the different data sources across the bank, by considering all the different stages of the transaction, but also interaction with the account. For example, coupling entitlement data with log in data will create a pattern of where somebody usually logs in, and when. Anything outside of that pattern may not necessarily be suspicious but will contribute to the overall risk scoring of the transaction.

It should be noted that by pulling the data together, it creates other issues that banks need to be aware of, specifically, data privacy and security issues. Any system is as strong as its weakest link and so there is a chance that it becomes a "point of failure" for the bank. Given how the data privacy rules vary by country, careful analysis will be required in the design of the system.

Technology

Given the disparate data sources and structures, the technology will increasingly focus on the ingestion of the data as much as the model itself. The data will need to be cleaned and reconciled, and increasingly there are advances in the technology to do so. It is likely that AI and Natural Language Processing (NLP) in particular will be used to link the data. This will be critical to ensure that there is a way to highlight discrepancies yet have an

acceptable level of false positives. In many cases, when the account details are updated, the account name is very similar to that of an existing one. For example, Celent U.K. to Celent UK. It has to be remembered that the fraudster will be very aware that obvious changes will more likely be noticed, and so will deliberately try to make the changes as subtle as possible.

The tools can then be used to make peer groups. While each corporation will be different, there will likely be some similarities between them. By creating a peer group, there is a control group and will improve the analysis by improving the modelling of expected behavior. Again, varying from that expected behavior isn't necessarily a flag in its own right, but adds to the overall risk score. It will also help identify patterns of transactions that may be suspicious. A single transaction may not be flagged, but similar single transactions across the peer group may stand out more.

Analysis

Given that banks have multiple touch points with corporations, they will have to have processes, procedures and technology in different parts of the value chain. For example, there are specific processes and technology that are associated with creating a new payee or amending an existing payee. Technology will already be playing a part for large value inbound payments under the bank's obligations for anti-money laundering regulation. Sharing as much information as possible between the applications will improve the results of all of the applications.

There are some common steps to all, however. At the heart of any solution will be data. Identifying the right data to analyze though is only part of the problem. Analytic models will need to learn or be taught what variables to do the analysis on. While data scientists will be able to build the models, subject matter experts will likely need to apply their knowledge to refine and improve those models. Understanding how clients work will be key to the success. In an ideal world, the analysis will be using data from multiple sources as well, both internal and external, so the team will include experts from across the business.

Central to the analysis will be understanding the behavior of clients as understanding what is normal may not be straightforward. Take a simple Payroll example. While most transactions will be made on the same day, to the same people, for the same amount, there will always be a turnover in staff. It is important then that the analysis can show that the new accounts being set up have been validated, so that it doesn't get flagged as suspicious. Vendor payments are more complex as many are not so predictable. Mapping the clients' vendor relationships and their prior payment history will be key. Domestic transactions will be easier to spot — indeed, they may bank the vendor — so there will likely be a weighting to look at international vendors. Here the focus will be looking across all the banks' clients to see if there are broader patterns. Data sources will also play a part, particularly in trying to identify account information for those vendors as well as data on how the transaction was initiated. For example, the coupling of the initiators log in details with their usual IP address of the device they use will give a view of the authenticity of the request. This is likely to get increasingly important. Client demands for improved accessibility and to be able to bank "anywhere, anytime" means that there is an increasing number of channels. Open Banking may make this yet more complex, but the digital "footprint" of a transaction provides significant insight into the transaction.

An important point to highlight is that these models cannot remain static but will need to continually evolve. While often longer-term plays, they are relatively cheap for the fraudster to execute in many cases and so can afford to pause particular attempts and/or change their approach. Given the returns, and very low number of criminals caught (as compared to other crimes), they are likely to be very inventive in their approach!

DEFEND

Detect is obviously a key stage in defending, but what should a bank do if it believes there is a suspicious activity? Rejecting the payment is one answer but there will be a risk of genuine transactions being caught as false positives. As a first step, many systems can be configured to generate alerts “in journey” at the client interface, highlighting the suspicions and risks, before the transaction is formally submitted for payment. Key here is that banks should agree with their clients’ specific operational procedures on how banks should respond. This ties in closely to education. Given that many of the frauds rely on pressure to do something quickly, ensuring staff understand that all pop-ups on their screen have a purpose, especially in fraud notification.

Should the transaction still be submitted, it is likely to require the bank to contact the client and to pre-determined people. After all, the bank doesn’t want to make the client think they are the fraudster. Equally, clients should let the bank know of key process changes or key personnel changes.

Once the bank has identified a suspicious transaction, it should then look through it’s data to see if any other activity has recently taken place, and, if so, notify those customers. Given the very targeted nature of many of the Authorized Frauds it is unlikely there will be any, but with frauds such as investment fraud, there is a greater possibility.

In an ideal world, the bank should contact its counterparty bank (that is, the recipient of the transaction) and notify them, as well as other large banks in their own country. Most large corporations are multi-banked in each country, and so it is possible that the client may have also made other transactions to the suspect but from accounts held at other banks. By alerting these banks that there is a potential fraudulent account, it allows those banks to check for suspicious activity as well. Fraud typically hasn’t been seen as a competitive differentiator for banks but highlighting to the client that you’re even proactively telling their other banking relationships may be a step in that direction. Given the scale of the problem, finding a way to proactively share concerns, in real time, would seem something that the industry as a whole would benefit from.

THE PATH FORWARD

Authorized Fraud is so widespread, and with such large sums being targeted, it should be on every bank's radar. The risks posed to their clients is sufficient that there is a risk to the bank itself in some cases. Yet there is also an opportunity to not just protect themselves and their clients, but to become the hero of the day. While banks obviously co-operate with the appropriate authorities, by taking a more proactive stance, they can help curb the level of fraudulent attempts in the first place. The estimate from the Treasury Department of 1,100 US businesses losing an average of $300 million per month also highlighted that 73% of those attempts came from a domestic fraudster. Banks could make a significant difference in reducing that number.

The efforts are unlikely to be quick, one-off projects. While there are quick wins possible, it will require ongoing efforts and investments to stay one step ahead of the fraudsters, yet there is great potential upside. It will require the bank to both invest in the necessary technology and accompanying processes, but also in a change in how they interact with their customers. Banks have traditionally focused on what makes them money rather than what might save the clients' money. As banks enter the post-Covid recession, building closer and deeper relationships with the clients will not only reduce churn, but will build relationships that are likely to be rewarding long term.

One of the key activities will be educating teams across the bank, and the role that they play in detecting the fraud. Simple changes in processes may have significant impact but will only work if the teams are aligned. A second, larger project is likely to be focused specifically on data. Banks have long spoken about the potential about analytics in payments, and so the need to address fraud may be the use case that drives the investment to make this happen.

This report was commissioned by Nice Actimize, at whose request Celent developed this research. The analysis and conclusions are Celent's alone, and Nice Actimize had no editorial control over report contents.

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman, Inc.

For more information please contact info@celent.com or:

Gareth Lodge glodge@celent.com

AMERICAS

USA

200 Clarendon Street, 12th Floor
Boston, MA 02116

Tel.: +1.617.262.3120
Fax: +1.617.262.3121

USA

1166 Avenue of the Americas
New York, NY 10036

Tel.: +1.212.541.8100
Fax: +1.212.541.8957

USA

Four Embarcadero Center, Suite 1100
San Francisco, CA 94111

Tel.: +1.415.743.7900
Fax: +1.415.743.7950

Brazil

Av. Doutor Chucri Zaidan, 920 –
4º andar
Market Place Tower I
São Paulo SP 04578-903

Tel.: +55.11.5501.1100
Fax: +55.11.5501.1110

EUROPE

France

1 Rue Euler
Paris
75008

Tel.: +33.1.45.02.30.00
Fax: +33.1.45.02.30.01

United Kingdom

55 Baker Street
London W1U 8EW

Tel.: +44.20.7333.8333
Fax: +44.20.7333.8334

Italy

Galleria San Babila 4B
Milan 20122

Tel.: +39.02.305.771
Fax: +39.02.303.040.44

Switzerland

Tessinerplatz 5
Zurich 8027

Tel.: +41.44.5533.333

ASIA

Japan

The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011

Tel: +81.3.3500.3023
Fax: +81.3.3500.3059