Identity crisis: Detecting account opening fraud in the age of identity commoditisation

Received (in revised form): 17th February, 2018

Uri Rivner
is recognised globally as an industry expert on cybercrime and advanced threats. Prior to joining BioCatch he served as Head of New Technologies, Identity Protection at RSA. He has worked closely with the world's largest financial institutions on developing solutions against online crime, phishing and Trojans, and helped other industry verticals establish an effective defence doctrine against advanced cyberthreats. He was a key player in developing anti-cybercrime technologies used today by thousands of organisations worldwide to stop billions of dollars in fraud each year and protect hundreds of millions of users.

VP Cyber Strategy, BioCatch, Yigal Alon St 126, Tel Aviv-Yafo, Israel
Tel: +972 544 497793; E-mail: uri.rivner@biocatch.com

Abstract Massive data breaches focused on stealing personally identifiable information (PII) have led to a world where identity data is a commodity. The level of account opening fraud in the financial sector and other sectors is growing at an alarming rate, as know-your-customer (KYC) checks are no longer stopping fraudulent online account opening. Traditional controls such as device reputation and geo-locational analysis become less effective as fraudsters fully understand that their access device and location is being monitored, and the industry is now attempting to establish a new defence doctrine against identity theft and account opening fraud. Tracking a user's digital identity in social networks and their interaction patterns as they open a new account are some of the next-generation tools that show promise in the fight for digital identities.

KEYWORDS: identity, identity theft, account opening fraud, new application fraud, cybercrime, synthetic ID, social media analysis, behavioural biometrics

INTRODUCTION

In mid-2017, the largest personally identifiable information (PII) hack in history exposed over half of the US population — with every piece of private information imaginable reaching criminal hands. The credit bureau that was compromised[1] is not alone: the last few years have seen major identity-related data breaches in other credit reference agencies,[2] data aggregators,[3] healthcare providers,[4] hospital networks,[5] federal personnel[6] and tax[7] authorities, as well as many other[8] global repositories for personal data.

Breaking into identity data vaults has a single purpose: identity theft. The stolen data is sold in the criminal underground, so that hundreds of cybercriminals can have an easy way of opening new accounts on behalf of unsuspecting ID theft victims. This in turns means that traditional know-your-customer (KYC) checks based on matching user data with known identity data repositories become redundant. KYC data is now a commodity: fraudsters have the data already. They can easily open a credit card, loan, mortgage or bank account; they can also open insurance, payroll, mobile service

or any other account that requires identity proofing. The victim will often find out about the identity theft when the collection team comes knocking on their door.

With traditional KYC checks no longer reliable, the most critical step in establishing a relationship between the user and its service provider — ascertaining the identity of the person — can be easily manipulated. This has far-reaching implications. Identity is under attack, and since identity is the basis for trust, authentication and authorisation, these are all in the line of fire. From onboarding a financial service to an eGovernment application to a blockchain node, without a way to ascertain identity, the entire value chain is at risk.

THE MAGNITUDE OF IDENTITY DATA BREACHES

Fraudsters obtain personal data such as Social Security number (SSN), name and date of birth through various techniques, such as randomly distributed phishing and malware, or hacking into identity data repositories. Hacking in particular has become so prevalent that identity data in itself can no longer be considered a secret.

One of the organisations tracking identity data hacks is the Identity Theft Resource Center (ITRC). According to ITRC,[9] in the first half of 2017 there were 791 data breaches in the USA, giving a projection of 1,500 breaches per year — well over the 1,091 reported in 2016 (see Figure 1).

It is important to highlight the difference between hacking into identity data repositories where highly sensitive, personal and unalterable data such as SSN, date of birth and credit history is stored, and stealing digital credentials such as user names and passwords. The former is typically used to open new accounts through identity theft, while the latter is normally used to take over existing accounts by playing the

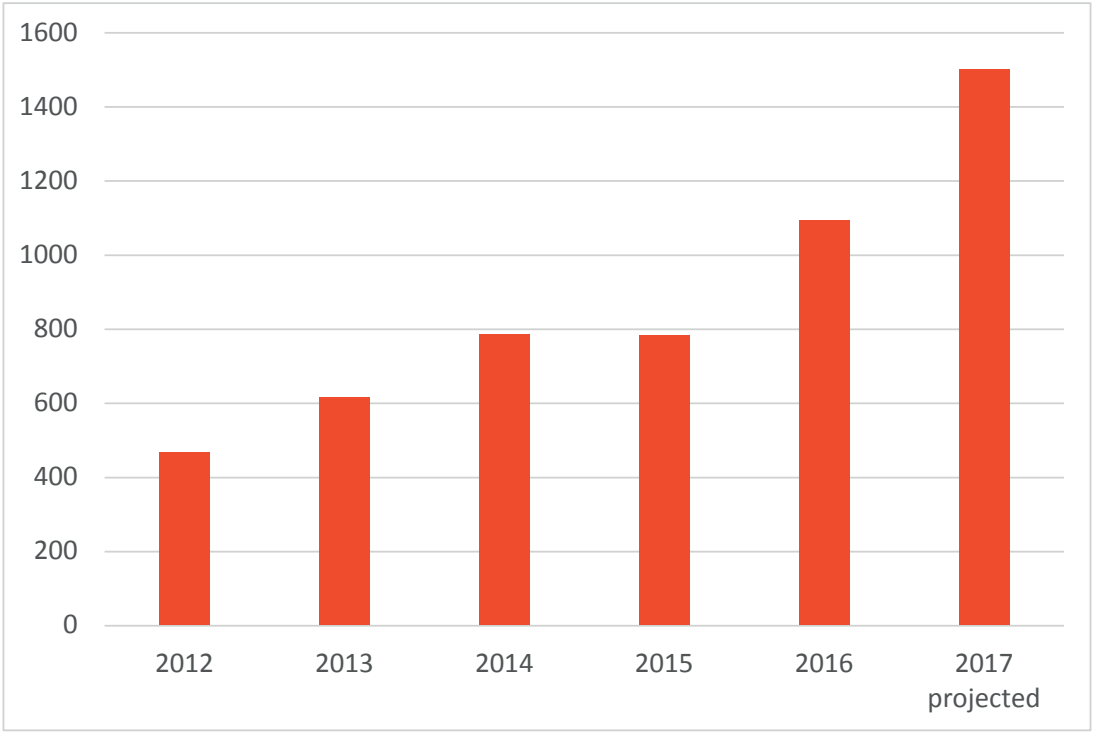

Figure 1: USA data breaches
Source: ITRC 2017 H1 Report

user–password combination on the original target and other websites (as people rarely use unique passwords per site). Hacks into digital credentials repositories are even more extensive than personal data breaches. The biggest breach to date occurred at Yahoo (3bn records), followed by Friend Finder Network (412m), MySpace (164m), eBay (145m), LinkedIn (117m), AOL (92m), Sony PlayStation (77m), DropBox (69m) Tumblr (65m) and Uber (57m). It should also be noted that the motivation for breaching many of those sites was stealing credit card data and conducting card-not-present fraud.

A SURGE OF ACCOUNT OPENING FRAUD

Using stolen personal information, fraudsters set up fake accounts that exploit weaknesses in the online account opening process. New account fraud is widely recognised as any fraud attempt that occurs within 90 days of the account opening. Credit issuers and digital payment providers are the most heavily targeted industries, but there are many ways a clever fraudster can utilise a fake account. On many occasions, the account is set up by a fraudster as a platform to carry out malicious and fraudulent activities.

The consumer database hacking in the USA, as well as the recent migration of credit cards to Europay, MasterCard and Visa (EMV),[10] have resulted in a dramatic surge in US account opening fraud. According to Javelin 2016 identity theft report,[11] account opening fraud in the USA increased by 113 per cent in 2015 — in other words, more than *doubled*. Account opening fraud in the UK is also on the rise, but more moderately: fraud increased[12] by 11 per cent in 2016, but this needs to be viewed in context of other metrics — for example, online banking fraud losses dropped 24 per cent due to the implementation of next-generation tools.

Credit card account opening fraud used to be a relatively small issue in the USA, but that is no longer the case; card issuers who have implemented EMV 'chip & PIN' report[13] growing ratios of both account opening fraud and card-not-present fraud, with account opening now responsible for 22 per cent of fraud losses for issuers with above-average adoption of EMV, second only to unauthorised transactions that account for 27 per cent of fraud.

An analysis of US consumer complaints related to identity theft shows a clear trend of growth in using stolen identity data to conduct account opening fraud. According to the Federal Trade Commission's consumer sentinel network report,[14] which aggregates about 400,000 US-based consumer complaints, the number of ID theft complaints involving a case where a new credit card account was opened under the user's identity jumped from 57,000 in 2015 to 102,000 in 2016 (see Figure 2).

The ratio of account opening complaints out of total complaints in the report is also on the rise: 25.6 per cent of identity

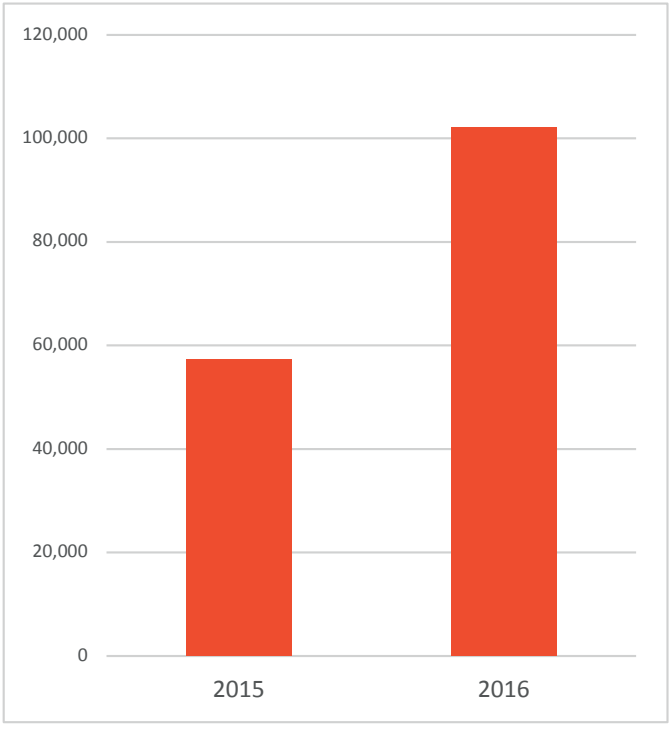

Figure 2: US credit card account opening fraud complaints
Source: FTC Consumer Sentinel Network Report

theft cases in 2016 were used in credit card account opening, up from 11.7 per cent in 2015. The same upward trend is true for opening utilities, mobile phone and bank accounts (see Table 1).The current magnitude of new account fraud is also apparent in the findings of AITE group research,[15] which places account opening at 47 per cent of fraud attacks on digital channels.

The motivation behind account opening fraud varies with the specific vertical:

- ***Credit cards and loans***: the fraudster attempts to open a credit account and then use it to buy sellable goods, or apply for a loan in which the funds are immediately available;
- ***Deposit accounts***: account opening fraud in banking is typically used for money laundering or for moving money out of compromised accounts in other banks without the need to use a 'mule';
- ***Utilities***: fraudsters may open utility accounts to receive free services;
- ***Mobile phones***: the fraudster will attempt to have the mobile device shipped to an address they control to sell it or use it in other fraud cases;
- ***Insurance***: a fraudster can buy a direct insurance policy with fake credentials and credit card details, then later make a claim;
- ***Payroll and tax***: a fraudster can open an online account for an employee who never had online access to date, then instruct the transfer of salary funds to a bank account they control, or send tax forms to an e-mail address they control;
- ***eGovernment***: a fraudster can file a requisition form, subsidies form or any other electronic government form that authorises access to funds or goods;
- ***Blockchain***: many organisations build blockchain-based networks that allow members to write data into the chain if they show proof of having their private key. Account opening fraud will strip away the level of trust in the blockchain and allow significant alterations.

Table 1: New account fraud out of total ID theft complaints in the USA

	2015	2016
Credit cards	11.7%	25.6%
Utilities	5.1%	5.6%
Mobile phones	3.7%	5.5%
Bank accounts	2.5%	4.3%

Source: FTC Consumer Sentinel Network

ACCOUNT OPENING FRAUD MOS

Fraudsters have two main modus operandi attack vectors when opening an account: *identity theft*, in which they take over an existing identity and open an account on the victim's behalf; and *synthetic identity*, in which they manufacture a completely fake identity. According to Lexis Nexis, 41 per cent of credit card account opening fraud involves identity theft, whereas 31 per cent involves a synthetic ID.

Identity theft

The main form of attack uses a stolen set of PII identifiers — in the USA data elements such as name, date of birth and SSN — to create a new account. The details go through a KYC validation process in which they are checked against credit bureau data or data aggregators; other data elements such as phone or address are also checked, but as they tend to change they cannot be used to verify a person.

Synthetic ID

A synthetic ID fraud starts from taking a SSN that has no credit record — eg SSN belonging to a 7-year-old — and inventing a whole new identity with a fake name, date of birth and other personal details. Since that identity is not real, there is no risk it will 'clash' with any true identity. What is left is to create a credit record for the new

identity: this can be done through collusion with rogue lenders or retailers who would do the identity equivalent of money laundering. The lender will ask for a credit report for the 'new applicant', receive a warning that there is no prior record, and then report that the person was actually given a chance to open an account and in fact they were a perfect customer, paying all their credit bills on time. The process is repeated until the synthetic ID gains a sufficient credit record and a good credit score. Another method is attaching the synthetic ID to an existing card account, in order to gain that account's tenure with the credit bureaus. In other words, the fraudsters manage to find the chinks in the armour and exploit the system to create a doctored record. Detecting synthetic IDs is very difficult as data checks simply cannot find anything wrong — everything matches, and no one is there to complain about their identity being compromised.

Robotic account opening

Websites are often attacked by bots who engage in mass registration of digital credentials (user name, password etc.). In contrast, using bots to open accounts that require the verification of PII is actually quite rare and tends to come in sudden, massive campaigns. The cybercriminals who stage the campaign may use either identity theft or synthetic ID records.

DETECTING NEW ACCOUNT FRAUD

Traditional KYC checks include matching the PII provided by a new applicant with the known record in their credit file or a similar data repository. But with identity data becoming a commodity, this is no longer a valid method for ascertaining one's identity. It is still a mandatory check due to anti-money-laundering (AML) regulation, but its effectiveness in catching fraud has deteriorated dramatically over the last few years.

Additional checks are run on information such as address, phone and e-mail. Do they match the ones on record for this user? How do all the various data points fit together? These are not very reliable checks, as the number of genuine people who have changed their address, phone and/or e-mail far outweighs the number of fraudsters.

Knowledge-based authentication (KBA) is one of the most predominant controls in account opening. KBA used to be almost a silver bullet against account opening fraud, but in light of all the stolen PII data, coupled with the fact that a lot of information on potential victims is available in open source content and social media, its effectiveness is dropping[16] and its use is on the decline.

Device recognition and network analysis can provide an additional insight. Unsophisticated fraudsters may use a virtual private network (VPN) service that has a proxy in New York while providing a San Francisco address; they can also use the same device to make hundreds of applications, or access from a device previously reported as the origin of fraud at another service provider — a fact that can be reported by *device reputation* services. Unsophisticated is the operative word here: the professional cybercrime rings are already familiar with device recognition and reputation services, which were introduced to the market circa 2004, and use an array of real or virtual machines, making sure to have enough entropy in their operation to confuse any device-related checks.

Industry detection rates of new account fraud in the credit card industry are not published, but can be gleaned off consumer surveys such as the one conducted by Javelin. According to the Javelin 2016 identity theft report, at least 25 per cent of ID theft is discovered by the victims themselves: 15 per cent of new account fraud victims discovered fraud through review of their credit report, and 13 per cent when they were contacted by a debt collector. This means that at least one out of four attempts is successful. The

actual number is probably much higher, but varies between verticals and individual service providers depending on how lucrative their business is and what sort of defences, operational procedures and risk appetite they have. Some service providers prefer to accept more applicants and see fraud as 'cost of doing business', while other service providers reject a number of applications if even the smallest of red flags is spotted.

What is clear is that both attempted and successful account opening fraud is on the rise, and the traditional methods are no longer holding. The KYC industry needs a new defence doctrine.

NEXT-GENERATION TECHNOLOGIES

Two types of emerging next-gen technologies go beyond the traditional KYC tools currently used by the industry and provide an orthogonal view on the risk factors of account opening: social media analysis and behavioural biometrics.

Social media analysis and e-mail characteristics

Analysing the digital footprint of a person in social media and open source content can reveal stark differences between the claimed identity and its actual digital presence. Based on the e-mail provided, how many social media accounts does this person have? Does this match the user profile — for instance their age? Young people would normally have an extensive social media presence, and this is a particularly vulnerable group as their credit history is quite thin. To beat the check, fraudsters will need to use compromised e-mail accounts: rather than use a fake e-mail account that will not match the real user's social media footprint, they can use a compromised account, access it before conducting the fraud and forward any notifications to another e-mail. This will make the fraud more complex, but not overly so, as hundreds of millions of compromised e-mail accounts are sold on the fraud underground.[17]

Social media analysis can be particularly effective against synthetic IDs, as fraudsters who want to be successful in their operation will also need to manufacture a fake digital identity and leave enough digital breadcrumbs to satisfy the social media analysis. This is not beyond the capabilities of cybercriminals, but it makes the crime less economical. It's not just about opening a lot of social media accounts — advanced data mining can also check if the people you're connected to are real, and how active they are in the digital space.

A more basic form of check is the age of the e-mail. Is this a recently opened e-mail, or does it have tenure consummate with the user profile? This check is easier to spoof, as 'grandfathered in' e-mail accounts opened years ago are on sale in the fraud underground.

Social media checks and e-mail address tenure provide an interesting new risk factor and can be considered a useful building block in a next-gen KYC defence doctrine.

Behavioural biometrics

A relatively new entrant to the KYC arena, behavioural biometrics technology tracks user interaction data — keyboard and mouse events for PC users, accelerometer and touch events for mobile users — and spots risky account opening cases by analysing the differences between genuine users who open accounts versus cyber gangs who conduct identity theft or synthetic ID campaigns.

Banks have been using behavioural biometrics for years[18] to protect existing users against account takeover. According to the federal Faster Payments Task Force, 'payment identity management (e.g., end-to-end encryption, tokenization, behavioral biometrics, and device fingerprinting) can and should be leveraged to protect data and stop fraud before it happens'.[19]

In its core, the behavioural biometrics technology builds a profile of the user's regular behavioural traits, interaction patterns and cognitive choices so it can spot intruders or threats in online applications. This will not work in an account opening scenario, though, as it's the first time the user accesses the application. Instead, behavioural biometrics refocuses its attention on the criminals.

Cybercriminals operate very differently from genuine, honest applicants. There are four key areas of difference:

Familiarity with the account opening process

Most fraudsters repeatedly attack the same application flow, as they have found a way to evade the existing controls. These actions show a fluency with the site and the process used to open a new account. A repeat offender will navigate quickly between fields, skip optional fields and interact faster with elements that would normally surprise a regular person. They will show a 'preparedness' level uncommon in genuine users.

In this example taken from a Top 5 US card issuer (see Figure 3), a behavioural biometric system flagged an online credit card application as high-risk. The user was extremely familiar with the application flow, interacting with it almost instantly, moving fast between fields and not showing signs of confusion in elements that normal people typically struggle with. The card company contacted the real person based on their last known phone number on credit bureau records, and they confirmed they did not try to apply.

Familiarity with the user's data

People are highly familiar with data elements such as name and date of birth; most of them are also familiar with elements like SSN. Fraudsters, however, are never familiar with victim data, and interact with each data element in a similar way. This creates very specific behavioural patterns.

To give one example, most normal people who are asked to provide their 5-digit zip code click on the field and instantly type the code. The zip code is in their long-term

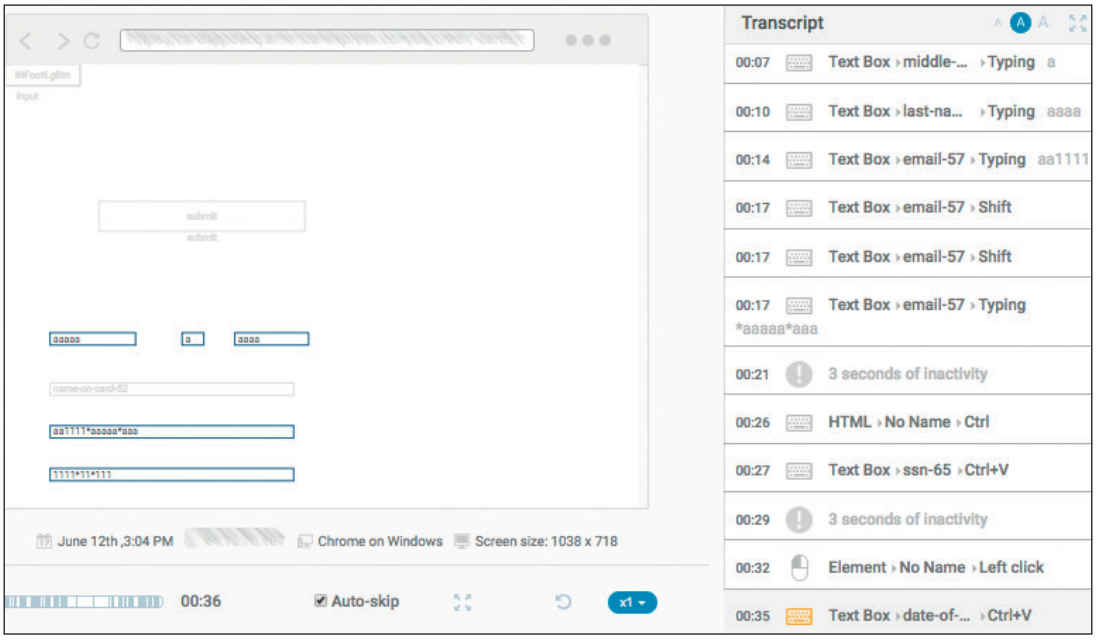

Figure 3: Behavioural biometric system

memory and the entry is essentially automated — US citizens are very used to the structure of typing their address, city, state and zip code. Fraudsters will not have the same familiarity and will normally reach the zip code field, consult with the victim list, and a couple of seconds later begin typing the code.

Another example is that of entering data that is not top of mind for most people — for example, their hotel chain loyalty number. A typical person who applies for a hotel chain credit card and is asked to provide the loyalty programme number will need some time to fetch it — but fraudsters are equally unfamiliar with all data points, be it personal (eg SSN) or non-personal (eg the hotel chain loyalty programme number). In this 4-minute 49-second online application process for a hotel chain credit card (see Figure 4), the user paused for about a minute to fetch the loyalty number; this is a positive signal, as fraudsters would normally provide the information at the same response speed as other data fields. Positive signals are important as they can 'clear' cases that are otherwise highly suspicious, such as a user mistyping their SSN so it clashes with someone else's data.

Computer savviness

A user who made a typo would normally click on the entry and correct it. Many fraudsters are extremely computer savvy and use efficiency shortcuts and combos; they often tab through the fields of a form, and in the case of typos they may use shift-tab to get back and correct the mistake. Of course, using shift-tab does not make one a criminal, but since only 0.13 per cent of legitimate users correct their typos with shift-tab, it is a good signal to use in a fraud detection model. The same is true for many other shortcuts and combos; mobile device data entry also has specific patterns that separate the 'power users' from regular people.

Unique criminal patterns

Tracking the behaviour of fraudsters who attempt to open new accounts can produce very clear behavioural patterns: these can be divided into generic and fraudster-specific. Generic patterns can include things such as typing contact e-mail and phone, which are normally not victim data but rather fraudster data, much faster than any other field. Specific patterns can get to the way a fraudster moves between certain fields, interacts with them, moves the mouse, scrolls up/down, presses on the touch screen of a mobile device, and holds it while opening the account.

FIGHTING ACCOUNT OPENING FRAUD — PRACTICAL CONSIDERATIONS

Fraud and risk managers responsible for account opening fraud can use the following list of questions to assess their risk policies and consider enhancing their defences:

- Is your account opening fraud volume growing year on year?
- Does your business team plan to add new, high-risk products that may be attacked by cyber gangs?

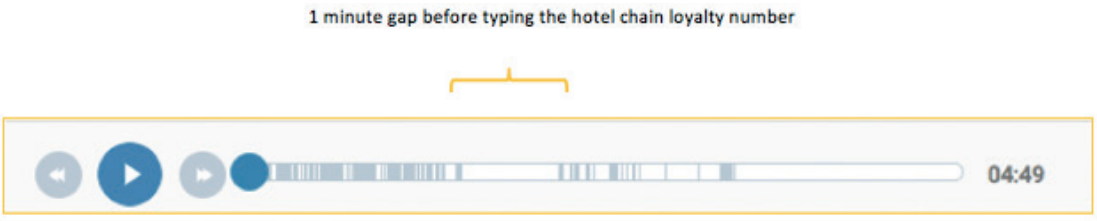

Figure 4: The 1-minute gap

- Does your business team push for automatically accepting more applications by removing controls with high false positives?
- Does your compliance team consider KYC checks based purely on data validation as sufficient, given the recent data breaches?
- What specific areas of the business are particularly vulnerable to attack?
  - Opening a new account online;
  - Registering to a web account for an existing user;
  - Adding a new mobile device for an existing account.
- There are two families of next-gen technologies: social media analysis and behavioural biometrics.
  - Do you know what solutions exist in those areas?
  - Is there a business case to test the effectiveness of such technologies in your environment?
  - Does your regular KYC provider offer any of those layers?

Conclusion

The industry is establishing a new defence doctrine against identity theft, synthetic identity schemes and other methods to subvert the identity-based economy. Traditional checks such as KYC, device reputation and geo-location analysis have been long compromised, and emerging tools such as social media mapping, e-mail tenure and behavioural analysis of the user interaction during account opening provide new visibility into criminal trends and show promise in fighting account opening fraud.

References

1. Tomberg, C., Dwoskin, E. and Fung, B. (September 2017), 'Data of 143 million Americans exposed in hack of credit reporting agency Equifax', *Washington Post*, available at https://www.washingtonpost.com/business/technology/equifax-hack-hits-credit-histories-of-up-to-143-million-americans/2017/09/07/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html (accessed 19th February, 2018).
2. Chabrow, E. (October 2015), 'Experian Hack Slams T-Mobile Customers', Bank Info Security, available at https://www.bankinfosecurity.com/experian-breach-a-8563 (accessed 19th February, 2018).
3. Krebbs on Security (September 2013), 'Data broker giants hacked by ID theft service', available at https://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service (accessed 19th February, 2018).
4. McNeal, G. S. (February 2015), 'Massive data breach at health insurer Anthem reveals social security numbers and more', *Forbes*, available at https://www.forbes.com/sites/gregorymcneal/2015/02/04/massive-data-breach-at-health-insurer-anthem-reveals-social-security-numbers-and-more (accessed 19th February, 2018).
5. Pagliery, J. (July 2015), 'UCLA Health Hack', CNN Money, available at http://money.cnn.com/2015/07/17/technology/ucla-health-hack (accessed 19th February, 2018).
6. McAllister, N. (July 2015), 'OPM Data Breach 21 Million People', The Register, available at https://www.theregister.co.uk/2015/07/09/opm_data_breach_21_million_people/ (accessed 19th February, 2018).
7. McCoy, K. (February 2016), 'Cyber hack gained access to more than 700,000 IRS accounts', *USA Today*, https://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/ (accessed 19th February, 2018).
8. McCandless, D. (February 2018), 'World's biggest data breaches hacks', available at (http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/) (accessed 19th February, 2018).
9. Identity Theft Resource Center (ITRC) (July 2017), '2017 Mid-Year Data Breach Report', available at http://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release (accessed 19th February, 2018).
10. Levy, O. (May 2015), 'Europay, MasterCard, Visa: a Primer', TechCrunch, available at https://techcrunch.com/2015/05/12/europay-mastercard-visa-a-primer/ (accessed 19th February, 2018).
11. Pascual, A. in Phillips Erb, K. (February 2016), 'Keeping Your Identity & Your Refund Safe from Fraudsters at Tax Season', *Forbes*, https://www.forbes.com/sites/kellyphillipserb/2016/02/12/keeping-your-identity-your-refund-safe-from-fraudsters-at-tax-season (accessed 19th February, 2018).
12. Financial Fraud Action UK (FFA UK) (2017), 'Fraud the Facts 2017', available at https://www.financialfraudaction.org.uk/fraudfacts17/ (accessed 19th February, 2018).
13. LexisNexis (June 2016), 'Lexis Nexis Card Issuer Fraud Study 2016', available at https://www.lexisnexis.com/risk/downloads/whitepaper/card-issuer-fraud-study-2016.pdf (accessed 19th February, 2018).

14. Federal Trade Commission (March 2017), 'Consumer Sentinel Network 2016 Report: January–December 2016', available at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf (accessed 19th February, 2018).
15. Inscoe, S. W. (November 2017), 'Digital Channel Fraud Mitigation: Evolving to Mobile-First', Aite, available at https://www.aitegroup.com/report/digital-channel-fraud-mitigation-evolving-mobile-first (accessed 19th February, 2018).
16. Kitten, T. (October 2017), 'Gartner's Litan on Fixing Authentication', Bank Info Security, available at https://www.bankinfosecurity.com/interviews/gartners-litan-on-fixing-authentication-i-2073 (accessed 19th February, 2018).
17. Reuters (May 2016), 'Hundreds of Millions of Email Accounts Hacked and Traded Online, Says Expert', NBC News, available at https://www.nbcnews.com/tech/security/hundreds-millions-email-accounts-hacked-traded-online-says-expert-n568491 (accessed 19th February, 2018).
18. Crosman, P. (November 2016), 'Next Gen Biometrics using the Force of Habit', American Banker, available at https://www.americanbanker.com/news/next-gen-biometrics-using-the-force-of-habit (accessed 19th February, 2018).
19. The US Path to Faster Payments report, July 2017 (https://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-task-force-final-report-part-two.pdf) (accessed 19th February, 2018).