CAPCO

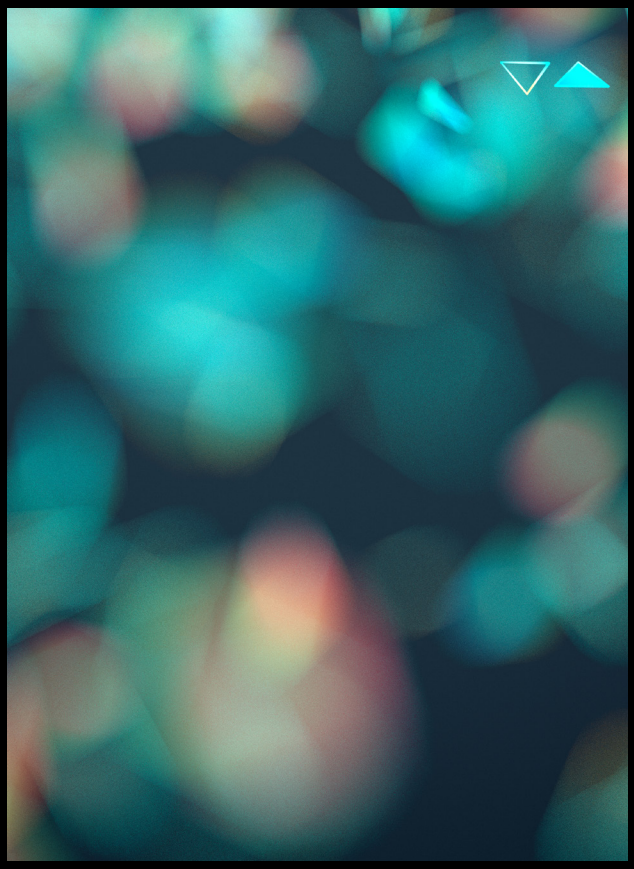
CYBER HYGIENE

HOW TO DISINFECT DIGITAL PAYMENTS AGAINST FRAUD

CAPCO

STEVENS INSTITUTE of TECHNOLOGY
School of Business

TABLE OF CONTENTS



CYBER HYGIENE: HOW TO DISINFECT DIGITAL PAYMENTS AGAINST FRAUD

For all the devastation that COVID-19 has wreaked worldwide, one impact has escaped widespread notice. COVID-19 accelerates payments attacks against financial institutions, consumers, and even companies as the pandemic changes buying habits and promotes a shift to remote work.

The pandemic has motivated consumers to rely more on contactless digital payments over cash as a hygiene measure. This contributed to a 32 percent increase in digital payments[1] at the start of the pandemic, although somewhat mitigated since the economy soured.

Another way to look at the payments shift is through the eyes of cybercriminals, who see a veritable greenfield in fraud opportunities, today and increasingly in the future as digital payment options proliferate. In April, Financial institutions (FIs) reported a 35 percent jump in dollar volume[2] of attempted fraudulent transactions year over year, according to Fidelity National Information Services Inc., known as FIS. And the head of cybersecurity for VMware told a House subcommittee[3] in May that cyberattacks against the financial sector rose by 238 percent between February and April, just as COVID-19 was gaining strength. The increasing use of remote workers only offers more exposure to employers struggling to update cybersecurity measures.

But COVID-19 is increasing a trend that was already prevalent. Over the last few years, several trends have converged to make cyberfraud more of a threat to institutions than ever. For one, fraudsters have become bigger, bolder, and more sophisticated—even several nation-states appear to be backing attacks on ATMs, FI databases, and skimming payment cards during brash point of sale attacks.

The story isn't just about bigger and better criminals, however. If Willie Sutton robbed banks because "that's where the money is," today, the money is everywhere: in transactions bouncing off of satellites, initiated on mobile phones, streaming through undersea cables, and in personal financial data stored on servers. According to the GSMA Mobile Economy Report 2018, 71 percent of the world's population could have access to digital payment technology[4].

The corporate shift to the cloud has opened an entirely new arena for hackers to play in, with massive breaches exposing tens of millions of accounts. And the tools of the trade cybercriminals use are better, too. An eye-opening spoof attack[5] in the United Kingdom last year used artificial intelligence (AI) and technology-enabled voice mimicry to convince a company employee to wire $243,000 into the account of thieves. The loss was relatively small potatoes among cyber exploits but a gigantic warning that fraudsters are once again upping their game and challenging the FI to respond.

Is there a path towards disinfecting digital payments despite current trends and the arrival of even more threats? We believe there is. By strengthening security around digital payments, hardening defenses in the cloud, and encouraging consumer-education campaigns, we see the foundation of cyber hygiene steps for building a resilient payments future.

WHERE ARE THE NEW THREATS COMING FROM?

Digital technology has created incredible opportunities for banks and other FIs to explore new business strategies and market opportunities. But digital technology also has armed criminals with new tools, such as AI and machine learning (ML), to create data breaches, trick consumers, and worm into what companies believed were secure data centers and payment processing programs.

To be sure, cybercrime was already on the rise over the past few years. One measure of increasing criminal activity has surfaced in cybersecurity breach disclosures. According to Audit Analytics (Trends in Cybersecurity Breach Disclosures, May 2020), there has been a 54 percent increase in breaches since 2017[6], a rogues' gallery of crimes including malware attacks, phishing, spoofing, and exploiting IT misconfiguration vulnerabilities. In this Year of COVID, however, it feels as if fraudsters are cashing in on the gift of chaos, and incidents will mutate even more virulently if not checked.

"We need to anticipate the specter of knowledgeable attackers gaining the sophistication to understand and deploy AI/ML capabilities, to make their attack attempts more scalable and lethal," argues Paul Rohmeyer, a financial cybersecurity expert who runs the FinCyberSec conference at the Stevens Institute of Technology. "Responding to AI/ML-driven cyber risks will create requirements for new skillsets, an understanding of how AI/ML can potentially manipulate vulnerable systems and personnel, and a focused observation on developments across the financial industry as these threats move closer to reality."

Fraud, of course, is as old as financial services itself. What is new is who is doing the defrauding and how they are doing it. Here is a glimpse at the new landscape.

NATION-STATE-SPONSORED ATTACKS

FIs had it relatively easy when they were battling individual fraudsters and teens with too much time on their hands. Now they even have to go up against rogue state-sponsored attackers.

North Korea, in particular, is believed to target payment systems and banking to raise funds to support weapons development. The country was implicated in the theft of millions in bitcoin and 'cryptojacking' computing resources to mine bitcoin. North Korea was also suspected of stealing millions from ATMs in Asia and Africa, and possibly made off with $81 million in a fraudulent SWIFT network transaction[7]. Given global sanctions taken against the country, coupled with its weapon development aspirations, expect North Korea to continue to invest aggressively in these types of attacks. According to an advisory[8] issued by the U.S. Department of State and other federal agencies in April, North Korea's "malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the integrity and stability of the international financial system."

Other state actors suspected of supporting cybercriminal activity include Russia, Pakistan, and China. Between March 1 and March 13, 2020, for instance, the largest number of targeted spear-phishing campaigns originated in China[9], according to cybersecurity operator Intsights.

CRIME IN THE CLOUD

After a slow start in early 2010, companies moved to the cloud at an amazing clip, including payment systems and data. The cloud brings obvious benefits to FIs, such as using automation to continuously updating cyber protection software. The cloud is also an ideal location to launch AI- and machine-based learning programs to detect fraud patterns and even deploy defenses as attacks are happening.

However, the consolidation powers of the cloud also mean that minor mistakes in the configuration of one area can amplify into a catastrophic loss. Even the most sophisticated cloud defenses may not be up to the challenge to fend off a criminal who uses psychology to fool employees to hand over the keys to the gold room. Most breaches can be tracked back to human error.

CASE STUDY:CAPITAL ONE AND THE $72 MILLION MISCONFIGURATION ERROR

Capital One was considered an antifraud poster child—until it was hit in 2019 with one of the largest cybersecurity crimes on record. A 33-year-old software engineer wormed her way into credit card applications left vulnerable by a misconfigured software firewall, allowing her to access a server where the credit applications were stored. The breach affected 100 million U.S. consumers, compromised 120,000 Social Security numbers, and exposed credit monitoring, offset by $34 million in insurance recoveries.

CREDIT CARD ACCOUNTS STOLEN IN POINT-OF-SALE (POS) BREACHES

It was thought (or maybe just hoped) that prevalent use of card chips in the United States would curtail POS breaches. But security surrounding these transactions remain vulnerable to skimming and other forms of attack. Sophisticated cybercriminals have learned how to suck out the purchase data and even record PIN entry at the store counter. Another approach is for fraudsters to infect a retailer's payment system with malware, collecting transaction data. That's what happened at a breach at Saks Fifth Avenue and Lord & Taylor[10] in 2018, affecting up to 5 million customers. The criminals used a phishing expedition to gain access through an employee's computer.

Expect adversaries to continue to focus on these vulnerabilities, given the easy payoff. Credit card fraud is no small problem. As the most common type of identity theft each year, reported dollar losses in 2019 were about $135 million[11], according to the U.S. Federal Trade Commission.

Changing consumer behavior caused by the pandemic is also likely to create more opportunities for cybercrime. We believe card-not-present (CNP) breaches will jump given increases in online shopping driven by the pandemic. According to research firm AITE Group, CNP fraud in the U.S. will total an estimated $5.9 billion this year[12], up from $3.2 billion in 2015.

B2B SCAMS TARGETING HIGH-VALUE TRANSACTIONS

Payment scams, of course, are hardly limited to the retail world, although retail is the primary focus here. It's worth noting that on the B2B payment front, increasingly sophisticated adversaries are going after high-value transactions such as wire transfers. In one of the more innovative attacks, pretexting was combined with AI to mimic the voice of a CEO with a slight German accent to authorize a quick wire transfer of $243,000[13] to a fraudulent location. This type of fraud will increase as adversaries hone their technical skills and add emerging technologies into their toolkits.

CASE STUDY: CHUBB LOSES $4.8 MILLION COVERAGE CLAIM IN SPOOFING ATTACK

In June 2014, an accounts payable employee at Medidata Solutions received an email purportedly from the company's president that ultimately led to her wiring $4.8 million to a fraudulent account. A subsidiary of Chubb Insurance refused to pay an insurance claim from Medidata, arguing that an attack on the insured's email system was outside coverage boundaries. The U.S. District Court in New York ruled against Chubb. "Medidata has demonstrated that its losses were a direct cause of a computer violation," the court ruled.[14]

MOBILE BANKING ATTACK

Most FIs offer mobile applications for customers to access their assets remotely. This trend has been reinforced during the pandemic when many banks shut their lobbies. According to the FBI, a 50 percent spike in the usage of banking apps has been observed since the start of the year.[15]

"The FBI expects cyber actors to attempt to exploit new mobile banking customers using a variety of techniques, including app-based banking trojans and fake banking apps," the agency announced in June. While mobile apps might appear to be secure on the surface, they are, in truth, vulnerable because they lack critical security features. Criminals have noticed, responding with fake banking apps and banking trojans, including MazarBot, BankBot, LokiBot and Anubis.

BUSINESS PROBLEMS FOR FINANCIAL INSTITUTIONS

Fraud losses—including losses linked to credit and debit cards—cost U.S. banks, merchants and cardholders $16.9 billion in 2019, up 15 percent from a year earlier and the highest amount since 2013, according to Javelin Strategy & Research[16]. Companies reporting the highest costs related to payment card and bank account breaches since 2013 were Equifax, $1.7 billion; Home Depot, $298 million; and Target, $292 million, according to Audit Analytics.[17]

But the ramifications for businesses or institutions targeted by payments fraudsters go way beyond money loss. Here are just a few shockwaves exploding out from a breach that can cause lasting damage.

Loss of investor confidence: A high-profile hit can turn a profitable quarter into a losing year, dragging down stock prices and investor confidence with it. After Target's breach , sales dropped 4 percent and its profit plunged nearly 50 percent the following quarter[18]. The share price fell 46 percent and the CEO resigned. Conversely, when Home Depot suffered a high-profile attack in 2015, proactive action and communication by the CEO not only limited damage in the stock market, the company added 25 percent in shareholder value[19] that year.

Brand damage: A corporate brand can take decades to build, but only a few news cycles to destroy following a data attack. In the United Kingdom, a breach at telecommunications provider TalkTalk resulted in the loss of 101,000 customers[20] after their private information was compromised, and they revolted on social media. A 2019 study by Radware[21] reported that 43 percent of companies that took part in the study experienced sour customer experiences and reputation loss due to a successful cyberattack.

Recovery burden: In the 12 months following a breach, small- and medium-sized companies faced, on average, $1.2 million in compromise costs and $1.9 million in business disruption costs in 2019, according to the Ponemon Institute[22]. Some other costs are incalculable, but still injurious. Consider the overall drain on corporate resources consumed with answering jammed support lines, communicating with vendors and key stakeholders, dealing with insurance companies and regulators, and putting out fires with institutional investors.

Liability issues: Who is liable when fraudsters pull off a payments heist? Traditionally, in CP cases, the bank issuing the card took the hit but now, the burden seems to be shifting to retailers. To escape that liability, merchants must install secure systems. Still, costly POS devices like Chip-and-PIN readers—an expense that already stressed restaurants and other shop owners find it difficult to pay. This is a hotly contested development that is far from settled.

CASE STUDY: COVID-19 PANDEMIC CAUSES INCREASE IN CYBER FRAUD

Millions of consumers have shifted their banking and purchasing activity to online channels since the coronavirus outbreak forced mandatory stay-at-home orders. Employees of most major businesses are also working from home full-time during the crisis.

The changes in e-commerce and mobile banking have created entirely new targets for hackers to exploit weaknesses in remote corporate networks, merchant e-commerce sites and financial institutions dealing with massive increases in mobile banking transactions. In February 2020, Lookout Phishing AI discovered a campaign that used SMS messaging to target customers to fake websites of well-known banks in Canada and the U.S., including Scotiabank, CIBC, HSBC, Chase and others. The campaign was designed to capture the banking credentials and login information of users.[23]

EFFECTIVE STRATEGIES TO CONQUER DIGITAL PAYMENT FRAUD

As we explored, digital payments crime is increasing and increasingly sophisticated trends like work-at-home promote a shift to digital payments. The good news is that improving technology such as AI is available to help conquer digital fraud, although the fix will also require ever-increasing vigilance by FIs themselves and significant help from consumers.

Here are actionable recommendations for FIs to follow beyond increasing the basic rules of cyber hygiene, such as motivating customers to frequently change strong passwords, use two-factor authentication, and rigorous rounds of software patching and keeping on top of security updates. The recommendations can be summed up easily:

1. Use intelligence to anticipate threats and mitigate loss
2. Reduce the attack surface internally and in the cloud
3. At POS, incentivize the use of Chip and PIN readers and tokenization
4. Educate consumers

USE INTELLIGENCE TO ANTICIPATE THREATS AND MITIGATE OR LIMIT A LOSS

In erecting barriers to the most sophisticated or powerful cybercriminals, especially those related to state-sponsored actions or B2B scams, the best mitigation is usually intelligence. Knowing who your adversary is, their likely methods of attack, and their motivations serve as the base for a threat intelligence-driven strategy.

There is a robust market for cyber threat intelligence, so it is widely available to payment processors and card providers. The difficulty for the FI is not intelligence, but rather the time to analyze the data and apply it to the threats facing the individual organization. Too often, this intelligence is unused, cast off to a deep corner of a remote data warehouse.

We believe FIs would be well served to build a capability around what is commonly called a Cyber Fusion Center (CFC). The CFC is the next generation of the Security Operations Center (SOC), which organizations have depended on historically to detect attacks and contain the damage. By contrast, the CFC extends well beyond this classic "moat and castle" defense.

Think of the Cyber Fusion Center as a platform that combines functions such as Cyber Threat Intelligence, Red Teaming, and Attack Surface Reduction, and makes them highly visible throughout the organization. To do so, CFCs integrate functions such as plant security, SecOps, and IT operations to promote more effective threat intelligence, creating a more proactive, collaborative, and unified approach to negating threats.

With a clear understanding of their own strengths and weaknesses, layered with actionable intelligence, FIs should set strategic and tactical priorities based on the actions and capabilities of their adversaries, their attack surface, and with a focus on the most critical payments systems and data.

But the old wisdom still stands when it comes to the basic blocking and tackling of cybersecurity: continually update your network security systems; partner with verified payment processors; keep on top of crime trends; ensure that tokens and login credentials are regularly changed, ensure your protections against internal threats are strong and embrace the many other hygienic basics you should already be following.

REDUCE THE ATTACK SURFACE INTERNALLY AND IN THE CLOUD

The boom in Internet-exposed assets from years of digital transformation, and accelerated by a seismic shift to a remote workforce in response to COVID-19 can make protecting your FI's digital attack surface feel overwhelming. FIs are responsible for defending their internal network and their digital presence across the internet and the cloud.

Bringing the enormous scope of an organization's attack surface into focus helps frame the challenges of extending cybersecurity outside the corporate firewall, especially as staff forced to work from home push that boundary farther out. One way to do it, is to red team the cloud and other pathways and blind spots that hackers are exploiting.

Red teams are a favorite tool of the military, and their task is simple: find flaws in the organization that can be exploited by the enemy. Red teamers, who report to and are supported by top commanders, are granted much leeway to act like insurgents and reveal vulnerabilities invisible to the rest of the organization. We think every medium- and large-scale organization should create a red team to attack itself using a three-tiered attack-and-discovery approach of 'outsider with no knowledge,' 'outsider with limited knowledge,' and 'an insider with knowledge' to provide a real-life test of their exposure to known security vulnerabilities.

But organizations need to do more to make sure they are organizationally prepared to block cyber threats. These include:

- **Incentivization.** Successful security is as much a mindset as a battle plan. The message must be pushed down from the top and accepted as part of the corporate ethos by every employee. Incentivize your team to get it right–"what gets checked, gets done."
- **Training.** Over half of all FI breaches are due to human error, especially in areas like support or customer service, where reps are more concerned with satisfying the customer than checking for security vulnerabilities. Invest in training and build systems that are resilient to user missteps. Special focus should be placed on senior leaders to heighten awareness of emerging threats.
- **Keep your software, hardware and cloud up to date.** Many hackers make a fine living off of companies who fail to keep security patches up to date or keep too much legacy or open-source software running in vulnerable areas. While pure cloud companies are usually well prepared for security maintenance, those that use the cloud but still rely on on-premise technologies can be vulnerable.

AT THE POINT OF SALE, INCENTIVIZE THE USE OF CHIP AND PIN READERS AND TOKENIZATION

Card payment fraud at POS continues to grow despite the fact that the industry now has the tools to put a serious dent into these crimes. The problem isn't the lack of technology, but rather consumer wariness over new technology and a slow-building tension between banks and merchants over payments liability.

Credit cards are invitations to steal for one simple reason: the information needed to make a card purchase—account number, expiration date, and security number—are all on the card itself. A fourth security measure, the zip code of the cardholder, is rarely requested at POS. Fraudsters can steal card information in many ways, including phishing, stealing database records, and skimming from card readers (See case study below).

Two technologies can lead the defense at POS transactions: Chip and PIN and tokenization. Unfortunately, in the U.S., too many merchants still accept cards with user information embedded on magnetic stripes, a technology from the 1960s. As a secondary check, retailers ask for the user's signature, scrawls that are rarely challenged. These technologies and procedures subvert the benefits of enhanced security provided by Chip and PIN.

Chip and PIN. Almost every credit card issued in the U.S. is equipped with an EMV chip, or "Europay, Mastercard, and Visa" technology, and many also carry a mag stripe as well. The cards come in two flavors: Chip-and-Signature and Chip-and-PIN. From a security standpoint, Chip-and-PIN is the gold standard and is used predominantly in Europe, where fraud rates are significantly lower than in the U.S. According to Barclays, the UK has fraudulent card transactions decline nearly 70 percent since adopting Chip and PIN cards.

However, Chip-and-Signature remains the preferred card type issued by FIs. Given the obvious security benefits, why is Chip and PIN not the standard in the U.S.? The catch for American consumers, some argue, is the inconvenience of having to remember and enter a PIN instead of just scribbling a signature. And for retailers, there can be additional costs associated with acquiring PIN devices, training staff, and educating users. For businesses like restaurants, which already operate on slim margins, the expense of installing dozens, hundreds, or even thousands of devices can be daunting.

Tokenization, simply put, is the process of exchanging a meaningful piece of data, like an account number, with a token or useless piece of information. When a consumer presents a tokenized payment card at the point of sale, the holder's primary account number is not exposed, so a fraudster has no incentive to go after the transaction. The information obtained, a random string of characters will be meaningless.

Also, The PIN is not stored on the merchant's device, servers, or the servers controlled by the digital wallet provider. First introduced in 2001, digital tokenization is proven, secure, and trusted. Tokenization is gaining popularity, at least by some card vendors. PayPal, Venmo, Zelle, Google Pay, and Apple Card, and Amazon Pay are examples of tokenized products.

We believe the U.S. must join with Europe, Canada, and most other developed nations to make Chip and PIN the standard retail payments device at the point of sale, and to support other products that use tokenization to enhance security. Fraud activity will diminish, and users will feel more secure.

CASE STUDY: 30 MILLION WAWA CUSTOMERS BREACHED

On December 19, 2019, popular grocery chain Wawa revealed a stunning breach. It announced that malware attached to payment card readers at "potentially all Wawa locations" had scraped off credit card and debit card numbers, expiration dates, and cardholder names on up to 30 million customers. The stolen data was later put up for sale on Joker's Stash , the internet's largest card fraud exchange. The company faces class-action lawsuits from consumers, financial institutions, and employees.

EDUCATE CONSUMERS

A primary goal of the financial industry is to move consumers to use more secure technology, such as mobile wallets and digital payments. Unfortunately, American consumers aren't on board. In an eye-opening Marqeta consumer survey , 80 percent of respondents stated, incorrectly, that a physical card is safer than a mobile wallet. At the same time, over half (54 percent) responded that the risk of fraud made them less likely to try newer payment technology.

But 77 percent of respondents did say they would choose to shop at a merchant who did not store their information in favor of one that did. Indeed, 75 percent said they would be willing to manually enter their payment information repeatedly rather than have it stored by a merchant, indicating that the extra one-time step of loading a payment card in a digital wallet would not be a hurdle if security benefits were better known. In other words, they embrace tokenization, even if they're not sure of what it is or how it works.

These attitudes mark a massive failure to educate consumers on how to make more secure payments by both the financial industry itself and technology companies who sell these products. For example, consumers worried about protecting their personal data and guard against identity theft should know that when a payment card is tokenized and inserted into a digital wallet on a mobile device like a smartphone or smartwatch, it loses its value for fraudsters.

CONCLUSION: IT'S A NEW DAY REQUIRING NEW WAYS

Digital payment systems are under attack as never before, a trend that the pandemic has only hastened as consumers change their buying behavior, and organizations face criminals with more sophisticated tools.

The sophistication of fraudsters is increasing—just look at the recent exploitation of flaws in the SS7 mobile data network that plays a critical role in directing traffic in most telecom networks. Metro Bank in the U.K. acknowledged last year that hackers were able to exploit SS7 to track phones remotely and intercept messages to authorize payments from accounts. Attacks on networks rather than on specific companies allow fraudsters to pull off massive breaches that affect millions of customers and cost companies millions in compensation, legal fees, and brand erosion.

Given these shifts in the threat landscape, it's no longer an option, if it ever was, for FIs to simply adopt a "moat and castle" defense, where the ramparts are raised in anticipation of an attack. FIs need to go on the offensive by investing in the latest technology, leveraging cloud protections, educating consumers and training their own organizations to be actively searching for threats.

"Attackers regularly recalibrate their objectives based on emerging technical vulnerability discoveries and in response to learning of successful attacks launched by others," says Paul Rohmeyer. "It is a never-ending cycle, and a sound cyber strategy must be informed by the prevailing threat and vulnerability landscape."

One door left unlocked is enough to results in millions in losses, many unhappy customers, and headlines that no CEO or investor wants to read. And even when COVID dissipates, the impetus it has given cybercriminals in 2020 will remain, perhaps to accelerate again on whatever disaster the next passing breeze brings us.

REFERENCES

1. https://www.aciworldwide.com/news-and-events/press-releases/2020/may/nearly-half-of-consumers-are-more-concerned-about-risk-of-payments-fraud-due-to-covid-19-crisis
2. https://www.wsj.com/articles/borrower-beware-credit-card-fraud-attempts-rise-during-the-coronavirus-crisis-11590571800
3. https://www.atmmarketplace.com/articles/cyber-fraud-surges-as-covid-19-changes-banking-e-commerce-2/
4. https://www.forbes.com/sites/danieldoderlein/2019/03/18/moving-towards-a-cashless-society-in-a-cash-reliant-world/#6a8cc82a236a
5. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
6. https://www.auditanalytics.com/doc/AA_Trends_in_Cybersecurity_Report_May_2020.pdf
7. https://www.pymnts.com/news/security-and-risk/2018/bangladesh-bank-heist-swift-phishing-scam-fraud-doj/
8. https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information
9. https://wow.intsights.com/rs/071-ZWD-900/images/Cyber%20Threat%20Impact%20of%20Covid19.pdf
10. https://www.marketwatch.com/story/saks-lord-taylor-data-breach-may-affect-5-million-customers-2018-04-01
11. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf
12. https://finance.yahoo.com/news/chips-credit-cards-dont-stop-fraud-online-200041701.htmlb
13. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
14. https://www.businessinsurance.com/article/20180706/NEWS06/912322505/Chubb-unit-Federal-Insurance-Co-must-cover-Medidata-spoof-email-loss-appeals-cou
15. https://www.ic3.gov/media/2020/200610.aspx
16. https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis
17. https://www.auditanalytics.com/doc/AA_Trends_in_Cybersecurity_Report_May_2020.pdf
18. https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031
19. https://www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf?utm_source=aoncom&utm_medium=storypage&utm_campaign=reprisk2018
20. https://www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf?utm_source=aoncom&utm_medium=storypage&utm_campaign=reprisk2018
21. https://www.radware.com/newsevents/pressreleases/2019/average-cyberattack-exceeds-1-million
22. https://www.keepersecurity.com/ponemon2019.html
23. https://www.atmmarketplace.com/articles/cyber-fraud-surges-as-covid-19-changes-banking-e-commerce-2/

CONTACTS

Julien Bonnay, Partner
E julien.bonnay@Capco.com

Bryce VanDiver, Partner
E bryce.vandiver@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

Bangalore
Bangkok
Bratislava
Brussels
Charlotte
Chicago
Dallas
Dusseldorf
Edinburgh
Frankfurt
Geneva
Gurgaon
Hong Kong
Houston
Kuala Lumpur
London
Mumbai
New York
Orlando
Paris
Pune
São Paulo
Singapore
Toronto
Vienna
Warsaw
Washington, DC
Zurich

WWW.CAPCO.COM

CAPCO