Griffith UNIVERSITY
Queensland, Australia
Griffith Criminology Institute

Card-Not-Present Fraud: Protecting Online Retail Businesses

Amanda Bodker, Phil Connolly, Oliver Sing, Benjamin Hutchins, Michael Townsley and Jacqueline Drew

Profit Protection
Future Forum (AU/NZ)

Overview

This report provides an introduction to card-not-present (CNP) fraud and the scale of this problem for the retail sector and its growing online sales channel. Drawing on a range of sources we provide a crime script detailing the steps involved in CNP fraud, discuss who the bad actors are, and the businesses at a higher risk of being targeted. After breaking down the problem of CNP fraud, we turn to practical steps businesses can take to protect themselves. This involves identifying critical steps in the crime script and providing recommendations on how businesses can use these as points of disruption. The report concludes with some general recommendations on broader practices to help businesses identify and respond to evolving threats in future.

Introduction

The online retail channel has grown steadily over the last decade. In the United States (US), e-commerce penetration increased 10% from 2009 to 2019, growing 1% each year. In 2020 the COVID-19 pandemic accelerated this trend, with evidence showing that in the first quarter of 2020, online sales penetration increased from 18% to 28% or ten years of growth in three months. More locally, Australia Post (2020) had previously forecast that online shopping would account for 16-18% of all Australian retail spending by 2025. Following the growth experienced in the first half of 2020, Australia Post re-evaluated this forecast, instead expecting online retail to account for 15% of the total market by the end of 2020. Such rapid growth in online retail, along with the speed at which many businesses are developing and expanding their online presence, is accompanied by increased opportunities for online fraud, particularly card-not-present (CNP) fraud.

CNP fraud entails the theft of valid payment card details and subsequent unauthorised use for transactions not requiring the physical card, such as those conducted online or by phone (Australian Payments Network, 2018) and is a significant problem. For instance, in 2019, CNP fraud accounted for the vast majority (85%) of payment card fraud occurring in Australia, with direct costs of $224 million on Australian-issued cards and $82 million on overseas-issued cards (Australian Payments Network, 2020). CNP fraud has remained the most prevalent variety of payment card fraud occurring in Australia, both on Australian- and overseas-issued cards, since 2014 (Australian Payments Network, 2020). These trends are consistent in other countries. For example, in the United Kingdom (UK), CNP fraud has been the most common subtype of payment card fraud since 2014 (UK Finance, 2020). During 2019, CNP fraud also accounted for the vast majority (76%) of payment card fraud occurring in the UK, with direct costs of £470 million.

How is CNP fraud committed?

Fraud itself can take place almost instantaneously with the current technology of online transactions. However, like all crimes, it is a process that requires special preparation and information before the fraud event itself. In addition, there are also steps that need to be taken post transaction that are necessary to realise the benefit of the fraud and evade detection. CNP fraud can be separated into three main stages: preparation (prior actions), doing it

(the transaction itself and receipt of goods), and getting away (after actions). Viewing CNP fraud as a staged process provides a means of identifying points of disruption at different stages of the criminal process. Figure 1 summarises this.

Preparing. Bad actors must first set themselves up with the knowledge and equipment required to commit CNP fraud in the preparing stage. In terms of equipment, online fraud is a low-cost, highly accessible offence. All that is needed is a computing device and internet access. Knowledge and skills are a more significant barrier, with many bad actors learning from tutorials in online forums and marketplaces on the dark web. Some of these forums implement security measures to prevent access by law enforcement agencies, requiring individuals to pass security checks, prove themselves, or have an existing member vouch for them before they can join. Once gaining access, these forums offer a range of services, including advice and tutorials on committing CNP fraud (and other online offences), security measures to ensure anonymity, markets to buy and sell stolen credit card details, and networking for contacts. Tutorials and information for basic skills are often free, however, more advanced tutorials require payment, typically in some form of cryptocurrency.

Once the required equipment and knowledge is attained, bad actors can begin offence specific preparations. One of the essential steps CNP bad actors take is their security measures to avoid detection by law enforcement. These measures range from basic steps such as deleting browser cookies before and after an offence, connecting to unsecured, open Wi-Fi networks, and using a virtual private network (VPN) to running virtual machines on virtual encrypted disks, media access control (MAC) address spoofing, using remote desktop computers and servers, and use of The Onion Router (TOR) browsers.

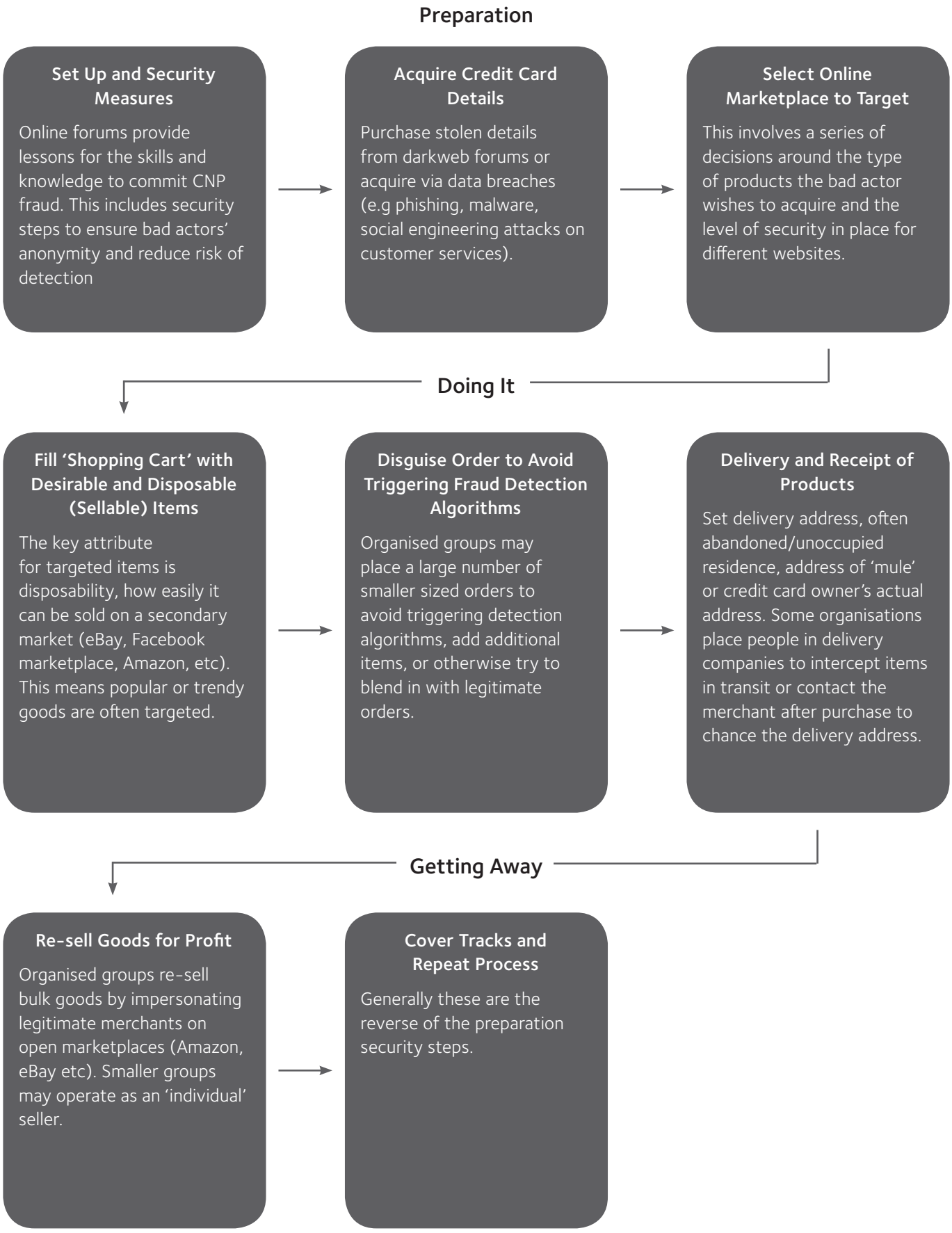
CNP bad actors need to obtain payment details to be used. This is achieved in several ways, including data breaches via phishing; identification theft; using social engineering to trick customer service representatives into providing information; placing someone inside the target business as an employee; or purchasing stolen credit card details from the dark web (Hutchings & Holt, 2015; Security Through Education, 2020). The final preparation step is selecting a suitable online store to target. This is determined by a combination of the merchant's security measures, company policies, the likelihood of merchants contacting the authorities if the offence is detected, and the types of products sold by the merchant (van Hardeveld, Webber, & O'Hara, 2016).

Doing it.

The next stage of the script is conducting the crime itself. It includes selecting products, disguising the order to avoid triggering fraud detection systems, the transaction itself, and delivery and receipt of goods. Several factors go into the decision-making process for the items bad actors target. However, one of the critical considerations relates to how easily a product can be on-sold. Bad actors will frequently target popular brands or products experiencing high demand (such as home office supplies during the COVID-19 lockdown)[1]. Once the desired goods have been selected, bad actors will often take steps to disguise the order to seem legitimate to avoid triggering fraud detection algorithms. This

[1]Gift cards are a popular target that has a slightly different process to other products. Gift cards purchased online are not physically delivered; rather the gift card details are provided instantly upon a successful purchase (i.e. without a delivery method). As a result, bad actors are able to use the gift card to purchase other goods or re-sell them before a merchant receives the chargeback from the cardholder.

Figure 1: A crime script of CNP Fraud



can involve making multiple fraudulent purchases across various merchants' websites (Lourenco, 2020b) and mimicking legitimate shopper trends to blend into traffic (either through a time of day for the transaction or items purchased). There is also some evidence that bad actors shop during busy holiday periods to avoid suspicion, though this has been disputed (Hutchings & Holt, 2015).

Once the products have been selected, bad actors enact the purchase with the stolen card details and set up delivery. There are various delivery methods bad actors choose to implement to avoid detection. Bad actors may provide a third-party delivery address, typically opting for express shipping. Express shipping is preferred as it allows bad actors to receive the goods quicker, the extra cost is not coming out of their pocket, and merchants have less time to determine if an order is fraudulent (Riskified, 2017). Alternatively, bad actors may provide the cardholder's address as the delivery location to lower the fraud detection risk score. Once the purchase is approved, bad actors will call the merchant to change the delivery address (Lourenco, 2020b). Alternatively courier services may be contacted directly to change the delivery address or method. While this seems simple, this can often involve a socially engineered script that manipulates the merchant's customer service employees into changing the delivery address (Lord, 2020). Organised bad actors may hire a (often unsuspecting) 'mule' to collect the package and deliver it to another address. Other, more resourceful organisations sometimes place people inside shipping companies as employees to intercept fraudulent orders and redirect them (Lourenco, 2020b). Buy Online Pickup In Store (BOPIS) is a newer 'delivery' method that is becoming a common avenue for fraud, with a 55% increase in 2019-20 (Fraud Attack Index 9th Edition, 2020).

Getting away.

The final stage of the CNP fraud crime script is getting away. These steps occur directly after the crime event and consist of post-offence security steps and post-offence steps to profit. Post-offence security steps generally involve the reverse of the preparation set-up steps: clearing cookies from web browsers, disconnecting VPNs, erasing virtual encrypted disks, etc. The final step in the script is re-selling the fraudulently purchased goods for profit. This is often done through marketplaces such as eBay, Amazon, or Facebook marketplace. Some larger organised fraud groups will impersonate legitimate businesses or suppliers to re-sell their goods in bulk.

Who commits CNP fraud?

Most CNP fraud involves stolen card numbers or account theft (Australian Payments Network, 2020). Online forums provide a means for individuals to develop their skills and network of contacts over time. While individuals can commit CNP fraud, they are generally executed by organised, transnational groups that form when these established individual offenders become core members. Depending on the skillsets these core members possess, they may subcontract the CNP fraud commission process elements to other individuals and/or groups (Nguyen & Luong, 2020). These organised groups usually operate in a different jurisdiction from where the CNP fraud occurs, which, combined with the practice of subcontracting elements of the fraud to non-group members, makes it more difficult for law

enforcement to counter (Australian Criminal Intelligence Commission, 2020).

Innovations in organised CNP fraud techniques tend to appear in the US initially and migrate to Europe before appearing in Australia after approximately six months. For Australian retailers, this is good news as it provides a significant lead time to adapt (Champion et al., 2019).

What are the likely targets of CNP fraud?

As with many crimes, fraud is difficult to measure accurately due to offender efforts to disguise their activities and inconsistent reporting of detected offences. The best available data source for quantifying and understanding CNP fraud methods are (a) chargebacks[2] and (b) transactions flagged by fraud detection systems. These data sources are not perfect, chargeback data includes both card-present and CNP transactions as well as legitimate and illegitimate chargebacks. Still, they can serve as a proxy measure of the problem.

Financial institutions classify businesses by Merchant Category Codes (MCCs), a four-digit number representing the types of goods or services they provide (e.g. 5942 is the code for book stores, 5072 is hardware equipment and supplies). MCCs can be classified into high-, medium- and low-risk based on several factors, but one of the key determinants is the magnitude of chargebacks relative to successful transactions (PayPrin, ND).

The retail MCCs most commonly classified as high-risk include;

- telecommunications equipment and sales;
- drugs, proprietaries, and sundries (wholesale);
- pharmacies;
- direct marketing, catalogue merchant, mail/telephone order; and
- tobacconists (includes e-cigarette/vape products)

Using detected fraudulent transactions, it remains true that a considerable proportion of fraud can be attributed to a small number of verticals. Juniper Research (2020) found that while airlines and money transfer industries account for the majority of fraudulent transactions by volume (62% collectively), retail verticals feature prominently with computers/electronics (13%), general retail (9%), clothing (5%), toys (1%) and jewellery (1%). The Forter/MRC Fraud Attack Index (Forter & Merchant Risk Council, 2016) observed that, for 2016, the apparel sector ranked first in terms of fraudulent orders (both successful and unsuccessful), with annual averages of $8.16 in every $100 of sales in the US, and $14.45 in every $100 of sales internationally being at risk of fraud (includes both successful and unsuccessful attempts). For the same year, the luxury goods sector ranked second with annual averages of $2.11 in every $100 of sales in the US, and $6.92 in every $100 of sales internationally being at risk of fraud; the electronic goods sector trailed just behind in third with annual averages of $2.04 in every $100 of sales in the US, and $6.44 in every $100 of international sales being at risk of fraud (Forter & Merchant Risk Council, 2016).

Research also demonstrates that some goods within a merchant's inventory are significantly more likely than others to be targeted by bad actors. According to Riskified (2016a), watches,

[2] When stolen card details are used to purchase goods, the account holder will not recognise that transaction and raise this with their bank. This is likely to result in a chargeback, "...a form of consumer protection where a card company or bank requests a charge from a merchant to be reversed" (Big Commerce, ND). Chargebacks are often associated with CNP fraud but are distinct and not strictly necessary for CNP fraud. Chargebacks are, at best, a proxy measure of CNP fraud. It is estimated that 75% of chargebacks are related to fraud.

sneakers, and jeans demonstrated higher fraud rates of 10%, 6% and 3%, respectively; by comparison, non-athletic shoes, jewellery, and underwear showed lower fraud rates of approximately 1%. A case study of a consumer electronics retailer conducted by Ethoca (ND) found that smartphones, tablets, and portable action cameras sold online remain frequent targets of bad actors. In addition to targeting particular goods, bad actors target specific brands, typically those considered "trendier" brands. Concerning sneaker brands, 'Nike Lebron', 'Timberland' and 'Supra' experienced the highest rates of fraud (43%, 40% and 23% respectively) while 'Converse', 'Asics' and 'Saucony' experienced significantly lower fraud rates (10%, 9% and 5% respectively; Riskified, 2016a). Looking at perfume sales, more popular fragrances such as Tom Ford and Creed appear to be more regularly targeted by bad actors, with these brands exhibiting below average safe approval ratings, almost 20% lower for the former and just over 10% lower for the latter (Riskified, 2018).

The consistent explanation for this distribution of CNP fraud is relatively simple; bad actors tend to target those goods for which there is strong demand, making them much easier to re-sell and realise a profit[3] (Ethoca, ND; Forter & Merchant Risk Council, 2016; Riskified, 2016a, 2016b, 2017, 2018). This hypothesis parallels the recommendations of Montague (2011), who advises those businesses selling goods of greater 'fenceability' (electronics, clothing, toys, mobile phones, etc.) to utilise more extensive fraud prevention measures because of their heightened risk exposure.

How can businesses protect themselves from CNP fraud?

With the continuing trend towards increased growth in online retail, it is vital for businesses to consider the risks and how to protect themselves. The preceding sections outlined how CNP fraud is committed, who commits it, and some of the standard targets to understand the CNP fraud process. The following section outlines a range of steps that can be used to disrupt this process and help reduce the risk of CNP fraud occurring. They range from simple measures any business can implement to interventions by government and law enforcement activity. These recommendations are discussed in order of the stages of the crime commission process they target: preparation, doing it, and getting away with it.

Preparation

Online forums and marketplaces on the dark web are invaluable for bad actors, providing much of the foundational knowledge and skills necessary for offending. Unfortunately, there is little that can be done to disrupt these, aside from the ongoing monitoring and shutdown of these sites by law enforcement, a process similar to a game of whack-a-mole. Transactions on these forums and marketplaces, however, almost exclusively use cryptocurrency. While cryptocurrencies provide varying levels of anonymity, traditionally the way they operate using blockchain allows all transactions to be traced, and networks of interacting users identified through clustering, potentially allowing law enforcement agencies to identify and disrupt users of dark web forums

[3] Extensive criminological research has demonstrated that crime is not equally distributed across all places, times, and people. This pattern extends to larceny, where a subset of goods typically account for a disproportionate amount of theft (Clarke, 1999). The targeting of these 'hot products' by thieves is best explained by the CRAVED theft model, which states such products tend to be Concealable, Removable, Available, Valuable, Enjoyable, and Disposable (Clarke, 1999). Though initially conceived to explain theft occurring in a physical environment, the model has also been applied to e-Commerce crime. Newman & Clarke (2011) posit that online auctions and secondary markets such as eBay and Amazon provide ample opportunity for stolen property to be disposed of. In this sense, one element of the CRAVED theft model – namely, that hot products are 'disposable' – demonstrates its efficacy in explaining the types of products typically targeted in CNP fraud (Newman & Clarke, 2011).

and marketplaces. As awareness of blockchain analysis tools increases, new cryptocurrencies (such as Monero) are finding ways to circumvent these tools of analysis. The differences in the properties of various coins make certain ones more appealing to bad actors, highlighting the need for fraud detection and analysis strategies to remain aware of these evolving trends in payment methods. As tracking and detection methods evolve, offenders may often be displaced to other cryptocurrencies that stay ahead of these methods. Cryptocurrencies also still have limited day-to-day uses, particularly in Australia, where few companies currently accept it as a means of payment (though this is changing). This means people dealing with cryptocurrencies need to use on-ramps and off-ramps to convert between cryptocurrency and fiat currency, allowing authorities to monitor for anti-money laundering (AML) purposes.

The vast majority of CNP fraud involves stolen credit card details or account theft acquired through data breaches. One precaution organisations can take to protect against data breaches is ensuring all software and systems are patched with the latest updates to defend against known vulnerabilities (Bossler & Holt, 2009; Hsieh & Wang, 2018). The Global Cyber Alliance (GCA) toolkit[4] provides a valuable guide for this process and recommends businesses keep an inventory of internet-capable devices, software/applications, and accounts and implement multifactor authentication and strong password procedures for both customer accounts and staff access. While software solutions provide protection from some data breaches and account takeovers, staff training to recognise other methods of data breach should not be overlooked. This should include recognising suspicious emails and phishing attempts, awareness of social engineering techniques used to target customer service staff, and clear processes on what to do in these situations (Jampen, 2020; Security Through Education, 2021). If a breach does occur, organisations should take steps to mitigate the damage immediately, including notifying affected customers, contacting relevant financial institutions, and reporting the incident to law enforcement. Some organisations may have requirements to report data breaches to particular agencies, such as the Office of the Australian Information Commissioner (OAIC).

The final recommendations for disrupting the preparation stage focus on measures businesses can enact to reduce the likelihood of being targeted by CNP bad actors. A good first step is ensuring policies regarding transaction processes and security measures are clearly stated and easily accessible on the website. Approaches could include measures such as not allowing delivery address changes after a purchase is made, ID and credit card verification to collect orders via in-store pickup, or reserve the right to hold orders for 24 hours before dispatching if deemed a fraud risk. By presenting the policy up-front and clearly explaining that it is designed to protect both the business and its customers, this step can deter would-be bad actors while explaining possible 'friction' legitimate customers may experience. This step can be taken further by advertising some of the security measures used to ensure that transactions are secure. Some examples of common security steps are the use of secure customer authentication (SCA) such as two-factor or multifactor authentication, using Payment Card Industry Data Security Standards (PCI-DSS) compliant service providers, or using a tokenisation service so that payment

[4] https://gcatoolkit.org

Figure 2. Points of disruption in the crime script for CNP fraud.

credentials details are not at risk in the event of a data breach (Australian Payments Network, 2020). Advertising the measures in place can increase legitimate customer confidence that their shopping experience will be secure. Lastly, retail businesses should continually evaluate and maintain a risk profile of carried inventory. This should be based on multiple sources of information such as trend reports from fraud control/payment networks and other companies, intelligence from the stolen goods market, and the organisation's own transaction data. While trend information from external organisations can be useful, there is no substitute for a business analysing their own data to identify products most at risk.

Doing it

Recommendations to disrupt the transaction process are essentially the last chance for businesses to prevent a CNP fraud attempt from becoming successful and are primarily dependent on well-designed fraud detection algorithms. Fraud detection algorithms use various methods but broadly analyse transactions for features that can indicate a high risk of fraud and flag them for more detailed review.

Standard risk features include:

- Orders originating overseas
- Unusually large orders
- Multiple orders of the same item
- A series of orders placed within a short time frame
- Use of a VPN or SOCKS5 protocol to mask location
- Inconsistencies in the order details (e.g. shipping and billing address do not match)
- Separate orders shipping to the same address but using different payment cards
- Orders shipping to multiple different addresses featuring the same billing address and payment card
- Multiple payment cards used by the same IP address

As discussed in the previous section regarding the targets of CNP fraud, there can be particular items that are at a higher risk of a fraudulent transaction. This is where the importance of businesses developing their own in-house inventory risk profiles becomes apparent. Augmenting the fraud detection algorithm with the inventory risk profile increases the likelihood of detecting fraud patterns specific to the business, rather than relying just on the experiences of other companies or aggregate data from fraud prevention providers that may have different processes.

Beyond simple detection of fraud attempts, it is also highly recommended that online retailers record all information of CNP fraud orders regardless of whether they are detected and prevented or approved and detected after the fact. This includes any contact information (names, shipping address, telephone numbers, etc.), associated payment details and chosen delivery method, as well as the items ordered. This information can be used to screen future orders for review if there is a match; for example, if an order matches the delivery address of a previous fraudulent order, it can be automatically flagged as a high-risk transaction. As the amount of information recorded increases, this should be used to update and refine fraud detection algorithms with the goal of reducing instances of rejecting legitimate orders or approving fraudulent orders. This is an important measure to counteract repeat offending in which bad actors re-target websites they have previously successfully

targeted. The ninth edition of the Forter Fraud Attack Index (2020) identified a 66% increase in repeat offending across 2019-20.

The final recommendations for this stage cover the various delivery methods. These can include the previously mentioned policy of not allowing the delivery address to be changed after purchase, or a policy of holding goods with an address change until extra verification steps can be taken (with the issuing bank, say). These measures would prevent social engineering tactics from diverting items from the cardholders' actual address to an address the CNP bad actor can collect. Internet Protocol (IP) geo-location checks can also be performed against the billing or delivery address provided, and if these do not match, follow up address verification steps can be taken. In the case of BOPIS, businesses should have a clearly stated (and strictly adhered to) policy of checking photo ID at collection.

It is worth pointing out that several factors operate that make strong control of deliveries problematic. Mandating signatures on receipt of goods is difficult when health authorities issue directives for contactless deliveries. Even though tracking numbers can serve to disrupt bad actors' attempts to intercept packages before they arrive at the original cardholder's address, many couriers make it straightforward to alter the delivery address or method directly.

If businesses experience delivery losses, it is critical to benchmark losses relative to the method or provider (or industry peers). This would provide insight into riskier delivery methods, flaws in the delivery process, or identify providers that are consistently associated with higher than average loss rates. This process will incentivise delivery companies to ensure secure and effective methods to make sure packages reach customers.

Getting away

The disruption points at this stage of the criminal process mainly relate to gaining information to minimise future losses and prevent bad actors from profiting. Still, at this point, the business has incurred some amount of loss. Nevertheless, we recommend retail organisations invest in the development of a dedicated chargeback resolution team. Such a team would analyse all instances of chargebacks to identify trends or patterns not just to prevent or dispute fraudulent chargebacks but also to protect customers and understand the causes of legitimate chargebacks so that these may also be reduced in future. This would provide valuable information that would design out opportunities for CNP fraud, ensuring a safer customer experience across the whole shopping process from browsing the online inventory, performing the transaction to shipping and delivery.

Developing real-time intelligence on stolen goods markets is an additional way that retailers could gain insight. Monitoring secondary markets and places of re-sale (such as eBay, Amazon, Gumtree, Facebook marketplace, etc) for missing goods or suspicious activity could be established as a surveillance system to provide insight into items or trends that can feedback into fraud detection algorithms. Further to this, it would be worth pursuing tax authorities to monitor re-selling sites for high volume accounts and their corresponding tax reporting obligations.

General recommendations

The above recommendations target particular parts of the CNP fraud crime script, but there are some general steps retail businesses can take to protect themselves. Anything cyber-related rapidly and constantly evolves, and cybersecurity prevention methods are routinely outpaced and superseded by offender innovation. Because of this, we strongly encourage business owners, loss prevention managers and cybersecurity professionals to seek out additional resources. There is a range of fraud solution services, both local and global, and while these companies offer paid services, many of them also provide free advice on their website or via mailing lists. These consist of tips on protecting your company, webinars on the latest e-commerce fraud trends, scams to watch out for, as well as articles and reports on the latest fraud protection technology. The Global Cyber Alliance toolkit is also a highly valuable guide that businesses should spend time familiarising themselves with and implementing.

Refunding fraud[5] is worth mentioning as one of the emerging ways bad actors are adapting to loss prevention methods and the broader online context. This type of fraud appears to be increasing substantially since early 2020, alongside the rapid growth in online sales brought on by the pandemic and the financial hardships that many people have experienced during this time (Chargelytics Consulting & Whisper Defense, 2020). This type of fraud is worth drawing attention to because it is not as easy to identify as the other types of CNP fraud discussed. Unlike CNP fraud, refunding fraud does not have an associated chargeback, and because they are initiated by the original cardholder using their actual details, they are not likely to trigger the fraud detection algorithms.

It is important to point out that underpinning all fraud detection and prevention systems are decision-makers who are human beings. Bad actors will continue to use social engineering tactics to thwart and circumvent the technological components of systems. Customer service teams should be seen as the last line of defence against bad actors; training that is effective and draws on the latest fraud practices is paramount.

The importance of collecting and analysing data on your customer shopping trends and any detected fraud attempts (both prevented and approved) cannot be understated. No other company will have as relevant data for the patterns your business may experience, and these should play an integral role in the development and implementation of fraud detection algorithms and customer policies. This process can be difficult, particularly for small businesses that may not have access to large amounts of data to identify patterns. This leads to our next recommendation that businesses pool de-identified transactional data to identify large-scale fraud detection patterns that may otherwise not be apparent. Retailers sharing this information will facilitate improvements in data security and education of social engineering and fraud methodologies leading to increased fraud detection and reductions in online retail CNP fraud. Turner (2020) states that there is no competitive advantage in an isolationist approach and that external collaboration, along with internal investment, can deliver more benefits utilising the sum of its parts.

[5] Where the legitimate cardholder makes a purchase and then contacts a professional 'refunder' who uses their knowledge of the policies and procedures of an organisation to get the consumer a full refund (while retaining the product/service) or a 'replacement' item (in addition to the received item; Chargelytics Consulting & Whisper Defense, 2020).

Reference List

Advanced Merchant Group. (2014, January 24). Card-not-present fraud: The basics. Retrieved January 12, 2021 from https://www.advancedmerchantgroup.com

Akram, J., & Ping, L. (2020). How to build a vulnerability benchmark to overcome cyber security attacks. IET Information Security, 14(1), 60-71. https://doi:10.1049/iet-ifs.2018.5647

Australia Post. (2020). Inside Australian Online Shopping2020 eCommerce Industry Report. Retrieved January 12, 2021 from https://auspost.com.au

Australian Criminal Intelligence Commission. (2020). Highest risk serious and organised crime. Retrieved December 29, 2020 from https://www.acic.gov.au

Australian Payments Network. (2018). Australian Payment Card Fraud 2018. Retrieved 12 January, 2021 from https://www.auspaynet.com.au

Australian Payments Network. (2020). Australian payment fraud 2020. Retrieved 12 January, 2021 from https://www.auspaynet.com.au

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. International Journal of Cyber Criminology, 3(1), 400-420.

Champion, D., Redfern, N., & White, A. (Presenters). (2019, June 27). The Australian Online Fraud Forum. [Audio podcast episode]. In N. Smith (Host), Retales: Conversations with Profit Protection. https://www.profitprotection.co/podcast/

ChargebackHelp. (n.d.). Merchant Category Code Index: Find your MCC. Retrieved January 5, 2021 from https://chargebackhelp.com/mcc-code-list/

Chargeback Gurus. (2020, February 21). Gift card fraud prevention 2020. Retrieved January 12, 2021 from https://www.chargebackgurus.com/blog/gift-card-fraud

Chargelytics Consulting & Whisper Defense. (2020). Fraud as a service refunding fraud-Merchants' new nightmare [Video]. https://www.youtube.com/embed/S4hOiTbtywg

Clarke, R. V. (1999). Hot products: Understanding, anticipating and reducing demand for stolen goods. London, UK: Home Office.

Cybersource. (2020). eCommerce fraud explained. Retrieved January 12, 2021 from https://www.cybersource.com/en-us/solutions/fraud-and-risk-management.html

EMB. (2017). High-Risk Merchant Category Codes – MCC. EMB. Retrieved January 5, 2021 from https://emerchantbroker.com/blog/high-risk-merchant-category-codes-mcc/

Ethoca. (n.d.). Case Study: Consumer Electronics Retailer. Retrieved January 12, 2021 from https://www.ethoca.com/

FIS Global. (2019). The best fraud prevention strategies for eCommerce. Retrieved January 23, 2021 from https://www.fisglobal.com/en/insights/merchant-solutions-worldpay

Forter & Merchant Risk Council. (2016). The Forter/MRC Fraud Attack Index. Forter. Retrieved January 12, 2021 from https://www.forter.com/reports/

Global Cyber Alliance. (2020a). GCA cybersecurity toolkit: Beyond simple passwords. Retrieved January 22, 2021 from https://gcatoolkit.org/smallbusiness/

Global Cyber Alliance. (2020b). GCA cybersecurity toolkit: Know what you have. Retrieved January 22, 2021 from https://gcatoolkit.org/smallbusiness/

Hsieh, M., & Wang, S. K. (2018). Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree. International Journal of Cyber Criminology, 12(1), 333-352. https://doi:10.5281/zenodo.1467935

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. British Journal of Criminology, 55(3), 596-614. https://doi:10.1093/bjc/azu106

Jampen, D., Gur, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. Human-Centric Computing and Information Sciences, 10(1), 1-41. https://doi:10.1186/s13673-020-00237-7

Juniper Research. (2020). Online Payment Fraud Whitepaper. Experian. Retrieved January 12, 2021 from https://www.experian.com/assets/decision-analytics/white-papers/juniper-research-online-payment-fraud-wp-2016.pdf

Kehl, F. (2020). Which Businesses & Industries Are Considered High-Risk? (& What It Means If You're On The List). Merchant Maverick. Retrieved January 5, 2021 from https://www.merchantmaverick.com/high-risk-business-company-industry/

Kount. (2020, November 5). What is Chargeback fraud? Criminal fraud vs friendly fraud. Retrieved January 12, 2021 from https://kount.com/blog/category/chargeback-prevention/

KPMG. (2020). Australian Retail Outlook 2020. Octomedia. Retrieved January 12, 2021 from https://home.kpmg/au/en/home/insights.html

Krebs on Security. (2019, June 27). Gift card fraud. Retrieved January 12, 2021 from https://krebsonsecurity.com/tag/gift-card-fraud/

Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. A. (2019). Criminal networks in a digitised world: On the nexus of borderless opportunities and local embeddedness. Trends in Organized Crime, 22(3), 324-345. https://doi:10.1007/s12117-019-09366-7

Lord, N. (2020, December 1). Social engineering attacks: Common techniques & how to prevent an attack. Digital Guardian. https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

Lourenco, R. (2020b, April 1). Fighting Organized Card-Not-Present Fraud. Risk Management. http://www.rmmagazine.com/2020/04/01/fighting-organized-card-not-present-fraud/

Lourenco, R. (2020a, January 9). Why gift card fraud is growing—and why the scammers are so hard to fight. Digital Commerce 360. https://www.digitalcommerce360.com/2020/01/09/why-gift-card-fraud-is-growing-and-why-the-scammers-are-so-hard-to-fight/

Maitlo, A., Ameen, N., Peikari, H. R., & Shah, M. (2019). Preventing identity theft: Identifying major barriers to knowledge-sharing in online retail organisations. Information Technology & People (West Linn, Or.), 32(5), 1184-1214. https://doi:10.1108/ITP-05-2018-0255

Martin-Vegue, T. (2015, June 24). Gift card fraud: How it's committed and why it's so lucrative. The State of Security. https://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/gift-card-fraud-how-its-committed-and-why-its-so-lucrative/

MerchantScout. (n.d.). High Risk MCC Codes: List of Merchant Category Codes categorized as high risk. Retrieved January 4th, 2021 from https://www.merchantscout.com/high-risk-mcc-categories

Montague, D. A. (2011). Essentials of Online Payment Security and Fraud Prevention (1st ed.). John Wiley & Sons Inc.

National Bank of Ukraine excludes WebMoney from register of inner-state payment Systems. (2018). https://112.international/ukraine-top-news/national-bank-of-ukraine-excludes-webmoney-from-register-of-inner-state-payment-systems-28810.html

Newman, G., & Clarke, R. V. (2011). Superhighway Robbery: Preventing e-commerce crime (1st ed.). Routledge.

Nguyen, T., & Luong, H. T. (2020). The structure of cybercrime networks: Transnational computer fraud in Vietnam. Journal of Crime & Justice, https://doi:10.1080/0735648X.2020.1818605)

Pannu, M., Gill, B., Bird, R., Yang, K., & Farrel, B. (2016, June). Exploring proxy detection methodology [Paper presentation]. 2016 IEEE International Conference on Cybercrime and Computer Forensic, Vancouver, Canada. https://doi:10.1109/ICCCF.2016.7740438

PayPrin. (n.d.). High-Risk Merchant Category Codes. Retrieved January 4th, 2021 from https://www.payprin.com/resources/high-risk-merchant-category-codes-mcc

Peretti, K. K. (2009). Data breaches: What the underground world of "carding" reveals. Santa Clara Computer and High-Technology Law Journal, 25(2), 375.

Riskified. (2016a). Fraud In Online Fashion: A Special Report for eCommerce Merchants. https://www.riskified.com/resources/report/2016-how-to-reduce-fraud-in-online-fashion-sales/

Riskified. (2016b). Fraud in Online Sneaker Sales: A Special Report for Online Retailers. https://www.riskified.com/resources/report/fight-ecommerce-fraud-in-online-sneaker-sales/

Riskified. (2017). Fighting CNP Fraud in Fashion: A special report for retailers. https://www.riskified.com/resources/report/2017-how-to-reduce-fraud-in-online-fashion-sales/

Riskified. (2018). The Beauty of eCommerce: Getting the Most Out of Online Cosmetics Sales. https://www.riskified.com/resources/report/the-beauty-of-ecommerce/

Security Through Education. (2021). The social engineering framework. Retrieved January 28, 2021 from https://www.social-engineer.org/framework/attack-vectors/vishing/

Shah, M., Maitlo, A., Jones, P., & Yusuf, Y. (2019). An investigation into agile learning processes and knowledge sharing practices to prevent identity theft in the online retail organisations. Journal of Knowledge Management, 23(9), 1857-1884. https://doi:10.1108/JKM-06-2018-0370

Soomro, Z. A., Ahmed, J., Shah, M. H., & Khoumbati, K. (2019). Investigating identity fraud management practices in e-tail sector: A systematic review. Journal of Enterprise Information Management, 32(2), 301-324. https://doi:10.1108/JEIM-06-2018-0110

St George Bank. (n.d.). Fraud prevention for merchants. https://www.stgeorge.com.au/content/dam/stg/downloads/business/merchant-support/Fraud%20Brochure%20SGB.pdf

Turner, J. (2020). CISO Lens benchmark 2020. Ciso Lens. https://www.austcyber.com/resource/ciso-lens-benchmark-2020

van Hardeveld, G., Webber, C., & O'Hara, K. (2016, May). Discovering credit card fraud methods in online tutorials [Paper presentation]. Workshop on online safety, trust and fraud prevention - ACM Web Science 2016, Hannover, Germany. https://doi:10.1145/2915368.2915369

Verifi. (2014). What every card not present merchant should know. What every card not present merchant should know