payments strategy forum

Financial Crime, Data & Security Working Group report

Draft for discussion: 27 June, 2016

"To engender user trust in safe and certain payments through collaboratively preventing financial crime."

payments strategy forum

Executive Summary

This paper provides an overview of the current financial crime education and awareness (E&A) landscape in relation to financial fraud.

Given the campaigns and messaging for current fraud / financial crime threats are already covered by existing E&A activities within the industry, the Payment Strategy Forum's Financial Crime Working Group has concluded that the priority therefore is for the payments industry / community to engage and support existing plans and activities. However, it is important that the industry enables a forward-looking component to its E&A plans with consideration for how best to pre-empt small but growing fraud MOs through early advice and messaging.

It is important to note that many organisations provide education & awareness advice; some directly to their customers and others to wider audiences for example, many third sector organisations undertake research and run fraud and scams awareness campaigns with particular focus on their target audiences. These organisations can be trusted messengers to communicate with hard to reach audiences, particularly the most vulnerable.

Acknowledging the busy landscape, the City of London Police, Economic and Cyber Crime Unit formed a multi-agency campaign group. The group aims to coordinate the development and delivery of Education and Awareness activity, and work towards simple, clear and consistent messaging so that audiences are not ultimately left confused. It also provides a mechanism for cross industry collaboration with the ambition of contributing to better use of finite resources in delivering these campaigns.

There are a wide range of financial fraud MO's that are used and which payments end-users (consumers, businesses, charities etc.) should be aware of. We have documented the priority areas, liaising across the PS Forum's Financial Crime Working Group. While the majority relate to fraud threats, we have considered the full scope of financial crime, for example we cover the issues of opening/operating mule accounts as a means of money laundering.

Table 1 below identifies high level campaigns that are already being undertaken to mitigate the effect of the priority threats.

Table 2 below outlines the key messages and advice being delivered through existing E&A activities.

A review of the effectiveness of existing activities will need to be undertaken to determine whether supplementary activity is required. The evaluation toolkit developed as part of the

UK Financial Capability Strategy may be useful in evaluating effectiveness and help to build evidence of what works which can then be applied to future activity.

payments strategy forum

Table 1

This table sets out the current financial crime priority threats where the Working Group advocates there should be customer education and awareness activity. The table also shows the existing E&A activity under way and the lead organisation.

Priority Threats	**Existing E&A activity/Lead organisation**
Social Engineering – several MOs employed Vishing Courier fraud Phishing Smishing SIM swap Investment scams Competition scams Romance scams Auction site scams Invoice fraud CEO Fraud	Take Five to stop fraud – Financial Fraud Action UK (FFA UK) & partners
ID Fraud	Not with my name - Cifas/CoLP
Money Mule Recruitment	Take Five to stop fraud - FFA UK & partners
Fraud associated with accepting card payments online	Mrs Norris - FFA UK/Cyber Streetwise
Malware, poor online safety behaviour and securing your online devices Mobile Banking Mobile payments (mobile technology)	Cyber Streetwise/Get Safe Online
Distraction card scams	Prevention advice via bank websites

Priority Financial Crime Threats and Key Messages

Table 2

This table shows the key messages for education and awareness, for each of the priority threats identified.

Threat	Audiences	Key Messages
Social Engineering Scams Vishing Courier fraud Phishing Smishing SIM swap Invoice fraud Investment scams Competition scams Romance scams Auction site scams	Consumers (all) Businesses	**Vishing / Courier Fraud** Fraudsters are increasingly targeting consumers over the telephone, posing as bank staff, police officers and other officials or companies in a position of trust. Often the fraudster will claim there has been fraud on your account and that you need to take action How to protect yourself: Your bank or the police will never: • Phone you and ask you to reveal your security information (for example your 4-digit card PIN or your online banking password) or request that you enter the information into a telephone. • Ask you to withdraw money to hand over to them for safe-keeping • Ask you to transfer money to a new account for fraud reasons, even if they say it is in your name • Send someone to your home to collect your cash, PIN, payment card or cheque book if you are a victim of fraud • Ask you to purchase goods using your card and then hand them over for safe-keeping If you are given any of these instructions, it is a fraudulent approach. Hang up, wait five

		minutes to clear the line, or where possible use a different phone line, then call your bank or card issuer on their advertised number to report the fraud If you don't have another telephone to use, call someone you know first to make sure the telephone line is free Your bank will also never ask you to check the number showing on your telephone display matches their registered telephone number. The display cannot be trusted, as the number showing can be altered by the caller **Phishing / Online** Phishing is a method used by fraudsters to obtain personal information from victims via email by impersonating a trusted person or familiar company. The email may contain malicious attachments or website links in an effort to infect the computer so that information such as passwords and personal information can be collected by the fraudster. The information collected will be used to commit fraud crimes such as identity theft and bank fraud. How to protect yourself: Ensure you have the most up-to-date security software installed on your computer, including anti-virus. Some banks offer free security software: check your bank's website for details Only shop on secure websites. Before entering card details ensure that the locked padlock or unbroken key symbol is showing in your browser Always be suspicious of unsolicited emails that are supposedly from a reputable

		organisation, such as your bank or the tax office and do not click on any links in the email Never share your personal or security information on a website that you have accessed by clicking a link in an email or text. **Smishing** 'Smishing' is very similar to 'phishing' but instead of using emails the fraudsters are using SMS text messages to your mobile phone. There are a number of variations on the scam which often starts with the fraudster sending an unsolicited text message within some cases the SMS contains a link, which if accessed can load malware onto your phone but more often will take you to a site where you are asked to enter personal and security information which will be used to defraud you. In most recent cases the customer is sent an SMS with a request to call a fraudulent number. When the number is called they are tricked into divulging security and possibly card details. A fraudulent transaction is then processed using the information provided and because the fraudster still has the customer on the line the customer is duped into releasing funds when they are asked to respond 'Yes' to a genuine SMS sent by the bank to validate the payment. • If you receive an SMS text from a sender that you do not know and are not expecting do not open any attachments or click on any links • If you receive a text from your bank asking for you to telephone them check the number, if in doubt phone the number on the back of your bank card or statement. **SIM Swap**

		This is when a fraudster cancels the SIM card linked to the victim's mobile phone and activates a new SIM card which is under the fraudster's control. This will allow the fraudster to re-route any calls and messages from the victim's phone and usually follows a phishing attack so that the fraudster already has the victim's bank account information: • If you stop receiving calls or text messages unexpectedly check with your phone operator immediately • Never disclose your PIN or internet mobile banking passcode in response to a SMS text - you would never be asked for the full four digit code or full internet/mobile banking passcode over the telephone • Be careful of the information that you add to social media sites such as your date of birth or maiden name and if possible use a different email address for social media than you use for contact with your bank and other sensitive applications. **Invoice Fraud** Ensure that all staff who process invoices and who have the authority to change bank details are vigilant. They should check for irregularities including changes to invoiced amounts Changes to supplier financial arrangements should always be verified with that supplier using their established on-file details When a supplier invoice has been paid, it is good to inform the supplier of the payment details made, including the account the payment was made to Check company bank statements carefully. All suspicious debits should be reported to your bank

		If you are suspicious about a request, ask if you can call back. Do so using their on-file contact details to establish if they are the genuine supplier of the services Perpetrators of fraud often conduct extensive online research to identify suppliers to particular companies. Consider if it would benefit your company to remove this information from your website / other publicly available materials Never leave sensitive materials such as invoices unattended on your desk Establish a designated point of contact with suppliers to whom your company makes regular payments. Raise all invoice issues and concerns with this person Consider a more vigilant strategy for larger invoices. A meeting with the supplier involved will ensure the payment is made to the correct bank account before the transfer is made Look carefully at every invoice. Counterfeit invoices won't often withstand scrutiny. Compare suspicious invoices with those you know are genuine Logos on counterfeit invoices often contain account details to which the payment should be made Be vigilant for amendments to contact numbers and email address on company invoices. Amendments to these may be so minor that they are difficult to spot Never accept invoice changes or new payment instructions via emails unless you first contact the designated contact that you know, often email accounts are hacked or fake email accounts that have one character different are used e.g. John.smith@ /

		John.sm1th@ **Investment scams** Investment fraud is often sophisticated and very difficult to spot. Investors are pressurised, into making purchase or sale decisions based on falsified information, often from an unsolicited phone call. Fraudsters can be articulate and appear financially knowledgeable. They have credible websites, testimonials and materials that can be hard to distinguish from the real thing People offering high risk investments or scams will often cold call. The firms that the FCA regulate are very unlikely to contact you in this way about investment opportunities. If you're called about an investment opportunity, the safest thing to do is hang up There are ways that callers can pretend they aren't cold calling you. They may refer to a brochure or an email that they have sent you. That's why it's important you know the other tell-tale signs that suggest the investment opportunity is likely to be very risky or a scam. Callers may do one or more of the following: • Make contact unexpectedly about an investment opportunity. This can be a cold call, email, or follow up call after you receive a promotional brochure out of the blue • Apply pressure on you to invest in a time-limited offer, for example, offer you a bonus or discount if you invest before a set date, or say that the opportunity is only available for a short period of time • Downplay the risks to your money, for example talking about how you will own actual assets you may sell yourself if the investment doesn't work as expected, or using legal jargon to suggest the investment is very safe

		• Promise tempting returns that sound too good to be true, for example, offer much better interest rates than those offered elsewhere • Call you repeatedly and stay on the phone a long time • Say that they are only making the offer available to you, or even ask you to not tell anyone else about the opportunity. If you recognise any of these, you have every reason to be suspicious If you have already or are thinking about transferring your pension, FCA strongly recommend that you do not send any more money. Find out more about pension scams on The Pensions Regulator website Not all investment opportunities offered out of the blue will be very risky or scams, but you should be very wary, especially if they are unusual investments. An investment offered to you in this way is unlikely to suit your specific needs and could be a very bad idea or a scam. It is generally best to seek out your own investment opportunities, either through research or with the benefit of impartial advice from a financial adviser **Competition Scams** A competition scam is when a victim is told that they have won a competition or overseas lottery and in order to 'claim' the prize which is usually something of high value, they must send money to cover a booking fee or the tax element on the overseas lottery prize money. • If you are asked to pay an up-front fee in order to receive a prize or winnings it is likely to be a scam. • If you do not remember entering the competition be sceptical, if you have received a letter try searching the exact name quoted on the internet to see if

		there are any references to a scam • If you believe the competition/lottery to be a scam do not respond, fraudsters will often use personal information they have gathered to play on the emotions of potential victims. **Romance Scams** These scams are often perpetrated through lonely hearts sites but can also occur as 'friendships' on other types of social media. The fraudster will build up a trusted rapport with the victim over a period of time and will take advantage of the victim's compassion to extort money through deception. **Auction Site Scams** A common scam occurs when the seller asks the buyer to pay the monies due by bank transfer directly into their bank account rather than using the auction site preferred settlement mechanism, often the reason given is to avoid the site charges or provide an additional generous discount. • Read the terms and conditions of the site very carefully especially those relating to dispute resolution before making any purchase • Beware of sellers offering discounts below the bid price especially as they want to trade outside of the auction site on which they are advertising. • Always check a website is secure before entering any kind of account or card details. Look for the 'HTTPS' at the start of the web address and the padlock or unbroken key icon at the top of the page or next to the address bar.
Money mule recruitment	Consumers: Students New entrants to UK	A 'money mule' is a person that will receive funds that have been obtained by criminal activity into their account and then forward those funds to other accounts, often overseas for a commission payment. Criminals will recruit 'money mules' to distance themselves from the crime and its proceeds. It is the 'money mule' that is taking the

		risk because they are committing 'money laundering', which can lead to up to 14 years imprisonment if found guilty. Behaviours that put you at risk: • Responding to job adverts, or social media posts that promise large amounts of money for very little work • Failing to research a potential employer, particularly one based overseas, before handing over your personal or financial details • Allowing an employer, or someone you don't know and trust, to use your bank account to transfer money. • Opening an account in your name for someone else to use How to protect yourself: • No legitimate company will ever ask you to use your bank account to transfer their money. Be very cautious of unsolicited offers or opportunities to make easy money • Be especially wary of job offers from other people or companies overseas as it will be harder for you to find out if they really are legitimate • Never give your financial details to someone you don't know and trust
Fraud associated with accepting card payments online	SMEs	**Know Your Customer** There are a number of tools and techniques which can be utilised when selling online to build up a profile of your customers Many of these can be working in the background as your website accepts an order from shoppers or when they first register on your site **Get Paid Securely**

		An important consideration for a merchant is to gain and validate a secure means of payment from your customers for the goods or services they are purchasing In the case of payment cards, as neither the card nor the cardholder are physically present at your business, it is vital to both validate the card number is genuine and authenticate that the customer is the rightful holder of that card **Internet cardholder authentication** Verified by Visa, MasterCard SecureCode and American Express SafeKey are authentication solutions offered to retailers and cardholders to assist in making internet transactions safer from the threat of fraud Retailers enrol into the service and make enhancements to the checkout process on their website Contact your acquiring bank or payment service provider (PSP) for more information about taking payments securely and internet authentication
Malware and poor online safety behaviour and securing your online devices	Consumers Businesses	**Firewalls** A firewall acts as a barrier between you and the wider internet including trusted and internal networks. Personal firewalls are usually software-based and should be installed on each computer which connects to the internet. However, firewalls for businesses may require hardware to protect their network further **Passwords** Make your passwords stronger with three random words. **Security Software** Security software such as antivirus helps protect your device from viruses and hackers

		Install software updates Software updates contain vital security upgrades which help protect your device from viruses and hackers **Create a safe wireless network** You should secure your wireless network (WiFi). Failing to do so could give someone else access to your sensitive data, including passwords or bank details, and use your network for illegal behaviour
Distraction fraud Card Scams	Consumers	When using your bank card be aware of people trying to divert your attention, perhaps by pretending to be helpful, dropping something or bumping into you so that they can take your card or cash, or find out your PIN. How to protect yourself: • Always shield your PIN when using your bank card • Always be aware of who is behind you when using your bank card and don't let anyone stand too close. • Don't let anyone distract you during the transaction • If anything about a cash machine looks suspicious don't use it. Tell a member of staff or the police

payments strategy forum