MEDIA STATEMENT - SABRIC ANNUAL CRIME STATS 2020

SABRIC, the South African Banking Risk Information Centre, on behalf of the banking industry has released its annual crime stats for 2020.

COVID-19, in conjunction with the implementation of regulations of the Disaster Management Act had a notable influence on financial crime trends in 2020. It triggered changes in human behaviour, human movement, and policing, creating new opportunities for criminals which significantly impacted the number of crime incidents. While some crime types decreased, others increased as criminals exploited COVID-19 for their own gain. Overall, SABRIC has seen an increase in banking crime incidents.

As customers turned to online shopping and settling payments on app, criminals enhanced their efforts to phish customers to steal their personal data to defraud them on digital and online platforms.

Digital banking fraud increased by 33%.

Debit card fraud rose by 22%, while on a positive note, credit card fraud decreased by 7%.

Contact crime was impacted by the restriction of movement and visible policing, resulting in a decrease in incidents. Associated robberies saw a decrease of 24% in 2020 when compared to 2019 with decreases evident in the Free State, the Eastern Cape and Mpumalanga.

While ATM attacks decreased by 9% overall, ATM explosive incidents increased by 20%.

Cash-in-transit (CIT) robberies decreased significantly due to the Level 5 lockdown in April and May of 2020, but once restrictions were lifted, these increased again by 22% as criminals were able to move with fewer restrictions and fear of roadblocks and searches.

Robberies and burglaries also increased by 42% and 12% respectively.

SABRIC CEO Nischal Mewalall stated: “Your personal data, when combined with technology has become the new key to the safe that holds your money in a bank, so you must safeguard your data to prevent criminals getting access to your safe.”

Mewalall further warned that looking ahead, cybercrime and data breaches will represent a significant threat to customers and banks, because even the best security and technology can be compromised when criminals source and use legitimate data illegally, to carry out a crime.

Mewalall also warns bank customers to never click on links in unsolicited emails as these links are used in phishing emails to drive people to "spoofed" websites which look like legitimate online retailers, complete with enticing images and convincing taglines.

"Criminals use these bogus websites to harvest bank card details to make online purchases using your account. We are still seeing lots of scam's advertising seemingly incredible deals for personal protective equipment, sanitiser and fake vaccines that exploit people's concern for their health and safety." adds Mewalall.

Please click HERE to access the SABRIC Annual Crime Stats 2020 publication.

[ENDS]

Be your money's best protection by following these **SABRIC tips:**

1. **Tips to prevent Card Not Present (CNP) Fraud**

- Personal information includes identity documents, driver's licenses, passports, addresses and contact details amongst others. Always protect your personal information by sharing it very selectively and on a need-to-know basis only.
- Never share your confidential information which includes usernames, passwords, and PIN numbers with **anyone**.
- Review your account statements on a timely basis, query disputed transactions with your bank immediately.
- When shopping online, only place orders with your card on a secure website.
- Register for 3D Secure.
- Implement dual authentication for all accounts and products, especially for financial services products.
- Do not send e-mails that quote your card number and expiry date.
- Do not use your information if you suspect it may have been compromised. Rather use other personal information that you have not used previously to confirm your identity in future.
- Register for SMS notifications to alert you when products and accounts are accessed.
- Conduct regular credit checks to verify whether someone has applied for credit using your personal information and if so, advise the credit grantor immediately.
- Investigate and register for credit related alerts offered by credit bureaus.

2. **Tips to prevent Phishing and Vishing**

Phishing:

- Do not click on links or icons in unsolicited e-mails.
- Do not reply to these e-mails. Delete them immediately.
- Do not believe the content of unsolicited e-mails blindly. If you are worried about what is alleged, use your own contact details to contact the sender to confirm.
- Type in the URL (uniform resource locator or domain names) for your bank in the internet browser if you need to access your bank's webpage.

- Check that you are on the real site before using any personal information.
- If you think that you might have been compromised, contact your bank immediately.
- Create complicated passwords that are not easy to decipher and change them often.

Vishing:

- Banks will never ask you to confirm your confidential information over the phone.
- If you receive a phone call requesting confidential or personal information, do not respond and end the call.
- If you receive an OTP on your phone without having transacted yourself, it was likely prompted by a fraudster using your personal information. Do not provide the OTP telephonically to anybody. Contact your bank immediately to alert them to the possibility that your information may have been compromised.
- If you lose mobile connectivity under circumstances where you are usually connected, check whether you may have been the victim of a SIM swop.

3. Tips for protecting your Personal Information

- Do not use the same username and password for access to banking and social media platforms.
- Avoid sharing or having joint social media accounts.
- Be cautious about what you share on social media.
- Activate your security settings which restrict access to your personal information.
- Do not carry unnecessary personal information in your wallet or purse.
- Do not disclose personal information such as passwords and PINs when asked to do so by anyone via telephone, fax or even email.
- Do not write down PINs and passwords and avoid obvious choices like birth dates and first names.
- Do not use any Personal Identifiable Information (PII) as a password, user ID or personal identification number (PIN).
- Do not use Internet Cafes or unsecure terminals (hotels, conference centers etc.) to do your banking.
- Use strong passwords for all your accounts.
- Change your password regularly and never share them with anyone else.
- Store personal and financial documentation safely. Always lock it away.
- Keep PIN numbers and passwords confidential.
- Verify all requests for personal information and only provide it when there is a legitimate reason to do so.
- To prevent your ID being used to commit fraud if it is ever lost or stolen, alert the SA Fraud Prevention Service immediately on 0860 101 248 or at www.safps.org.za.
- Ensure that you have a robust firewall and install antivirus software to prevent a computer virus sending out personal information from your computer.
- When destroying personal information, either shred or burn it (do not tear or put it in a garbage or recycling bag).
- Should your ID or driver's license be stolen report it to SAPS immediately.

4. Tips for protecting yourself against SIM Swops

- If reception on your cell phone is lost, immediately check what the problem could be, as you could have been a victim of an illegal SIM swop on your number. If confirmed, notify your bank immediately.
- Inform your Bank should your cell phone number changes so that your cell phone notification contact number is updated on its systems.
- Register for your Bank's cell phone notification service and receive electronic messages relating to activities or transactions on your accounts as and when they occur.
- Regularly verify whether the details received from cell phone notifications are correct and according to the recent activity on your account. Should any detail appear suspicious immediately contact your bank and report all log-on notification that are unknown to you.
- Memorise your PIN and passwords, never write them down or share them, not even with a bank official.
- Make sure your PIN and passwords cannot be seen when you enter them.
- If you think your PIN and/or password has been compromised, change it immediately either online or at your nearest branch.
- Choose an unusual PIN and password that are hard to guess and change them often.

5. Tips for Carrying Cash Safely

Tips for Individuals

- Carry as little cash as possible.
- Consider the convenience of paying your accounts electronically (consult your bank to find out about other available options).
- Consider making use of cell phone banking or internet transfers or ATMs to do your banking.
- Never make your bank visits public, even to people close to you.

Tips for Businesses

- Vary the days and times on which you deposit cash.
- Never make your bank visits public, even to people close to you.
- Do not openly display the money you are depositing while you are standing in the bank queue.
- Avoid carrying moneybags, briefcases or openly displaying your deposit receipt book.
- It is advisable to identify another branch nearby you that you can visit to ensure that your banking pattern is not easily recognisable or detected.
- If the amount of cash you are regularly depositing is increasing as your business grows, consider using the services of a cash management company.
- Refrain from giving wages to your contract or casual labourers in full view of the public; rather make use of wage accounts that can be provided by your bank.
- Consider arranging for electronic transfers of wages to contract or casual labourers' personal bank accounts.

To arrange interviews with SABRIC CEO, Nischal Mewalall, contact:

Louise van der Merwe
Tel: +27 11 847 3134
Cell: 082 070 5349
Email: media@sabric.co.za

Notes to Editors:

SABRIC is an NPF company formed by South African banks to support the banking industry in the combating of crime. SABRIC's clients are South African banks and major CIT companies. Its principal business is to detect, prevent and reduce organised crime in the banking industry through effective public private partnerships. SABRIC co-ordinates inter-bank activities aimed at addressing organised bank related financial crime, violent crime, and cybercrime, and acts as a nodal point between the banking industry and others, in respect of issues relating to these crimes. The creation of public awareness of various bank related crimes and educating the public on how to protect themselves is one of SABRIC's key focus areas. For more on SABRIC visit www.sabric.co.za.