URGENT BULLETIN

DATE:	April 16, 2020
AFFECTED PRODUCTS:	ALL CREDIT AND DEBIT
TOPIC TYPE:	Security
SUBJECT:	IMPORTANT NOTICE – Increased Phishing Fraud Attempts During COVID-19

SUMMARY

FIS™ continues to monitor and respond to the outbreak of COVID-19. As the backbone of the financial and commerce world, we are committed to maintaining the superior service you expect from FIS.

FIS and other financial organizations have seen an increase in phishing events during the COVID-19 pandemic. Phishing events are when a fraudster attempts to steal a person's data, mainly login credentials and card information. The fraudster then uses this information to process fraudulent card transactions or ATM withdrawals. Fraudsters often utilize social media or information bought on the Dark Web to initiate scams.

FIS ACTION

An example of the recent Phishing Attack:

- The fraudster gathers information from social media to make the scam more believable.
- Cardholder receives a phone call from the fraudster posing as a financial institution employee.
  - Fraudsters often spoof phone numbers from the financial institution when contacting the victim, making it seem legitimate.
- Fraudster advises cardholder that they have fraud attempts on their card and they will receive a text with a case number.
  - While on the phone, the fraudster will perform a transaction they know will generate a fraud alert
  - When the cardholder receives the case number, the fraudster asks for the case number over the phone so the card can be permanently blocked.
    - Instead the fraudster is using the case number to call into the SecurLOCK IVR and validate the activity as valid, so they can continue to use the card fraudulently.
- The fraudster may suggest the cardholder transfer money into their checking account from savings to make it "safer," thereby giving the fraudster access to more money.
- The cardholder thinks the fraud was caught and stopped, while the fraudster is busy committing more fraudulent transactions and stealing more money.

FIS will never contact the cardholder to ask for the following:

- Account Number/Card Number
- CVV
- PIN
- Passwords
- Social Security Number
- Online Banking Credentials
- Case Numbers

FIS will never advise a cardholder to transfer money or withdraw money. If any information concerning suspicious activity is texted to the cardholder, FIS does not call and ask the cardholder for the information. When cardholders call into SecurLOCK to validate suspicious transactions, FIS will request the case number to authenticate them. The cardholder should always reply NO if they are unaware of the transactions in question received via a text or email, no matter what direction has been given to them.