PAYMENT CARD BREACH LIFECYCLE

In the aftermath of a payment card breach, as fraudsters race to exploit the stolen information, card issuers and affected customers take steps to mitigate risks. The following looks at the lifecycle of a payment card breach from these three perspectives.

CARD ISSUERS		CONSUMERS
Receive notification from card brands that a compromise has occurred	1	Receive notification from their card issuer or credit monitoring service
Determine the name of the entity breached and initiate an investigation	2	Sign up for credit monitoring services (if not already using)
May engage a third-party service provider to monitor carder channels for the presence of bank-owned cards being traded in hacker marketplace; many banks now also monitor underground forums themselves	3	May opt for text or e-mail alerts to increase account awareness from their bank, credit union or retailer
Analyze historical transaction patterns to determine a common point of compromise with fraudulent activity reported by other issuers	4	Watch monthly statements for any suspicious activity
Determine if time range of the purported breach reported by the card brands is accurate, and that all of the issuers' cards exposed can be linked to the affected merchant	5	Receive new credit/debit card
Implement rules to prevent the breached population of cards from being used any further	6	May be further targeted via social engineering
Advise cardholders about suspected breach and plans to replace their cards; reissue cards to customers	7	Could change purchase behavior (stop using debit and adopt a credit card for purchases, stop shopping online or at a certain merchant)
Continue monitoring transaction activity to head off any additional fraud outbreaks	8	May return to the same breached merchant before the breach is under control, resulting in the compromise of their newly reissued payment card (because consumers are sometimes not told what merchant was affected)

Meanwhile, the **FRAUDSTERS**...

- Test stolen account data to determine if it is still valid for payments (known as "dump checking")
- Sort cards by issuing bank and any location-specific information, such as ZIP codes, so that "carders" can purchase inventory based on certain issuers and geographic locales
- Sell large batches of stolen account data to carders on a wholesale basis; card forums will even provide support services and guarantees that cards will work
- Prices can range from 75 cents to $20 per card, depending on the size of a payment card breach*
- Carders may need to further steal or assemble additional information, like CVV2, to make stolen card account data work in a card-not-present environment
- Encode stolen numbers on counterfeit cards and use for fraud, or simply perform card-not-present transactions that do not require a physical card
- Cash out by conducting fraudulent transactions (often via fraudulent merchant and bank accounts, as well as using ATMs)

For more insights about the underground economy and steps being taken to mitigate the use of stolen credentials, including payment cards, see:

http://www.databreachtoday.com/taking-down-underground-economy-a-6783

View this infographic online
http://www.databreachtoday.com/infographic-payment-card-breach-lifecycle-a-7812

Sources
FICO Card Alert Service, Ontrack Advisory

*According to research conducted by Juniper Networks

Data Breach
Prevention. Response. Notification. TODAY