Protect the Payment System from Account Testing and Fraudulent Authorizations

Stan Hui, Director, Fraud & Breach Investigations
Ed Verdurmen, Director, VisaNet Processor Risk

9 August 2016

Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Agenda

- What is Account Testing / Fraudulent Authorizations?
- Testing Trends
- Detecting, Responding and Reporting Testing Incidents
- Key Takeaways

What is Account Testing / Fraudulent Authorizations?

Why Account Test?

Threat actors test account numbers to validate cardholder information obtained through two main methods:

1. Data Breaches (POS malware or system intrusion)
2. Account Number Generators known as CreditMaster or CreditWizard

Once an account number is validated with an approved authorization, the fraudsters are able to monetize the cardholder information by selling it on the Dark Web.

- Accounts produced by CreditMaster, or more often stolen from files or databases, lack expiration date and sensitive authentication data such as CVV or CVV2
- Accounts stolen from POS devices using memory-scraping malware lack CVV2
- 3 and 4 digit numbers may be derived by simply trying all possible combinations (brute force testing)
- Brute force testing comes through acquirers in VE, LAC, AP, and CEMEA
- Test authorizations are rarely posted
- In a recent case, 40% of the test authorizations were reversed

Two Types of Testing

Brute Force

Used to derive additional card data elements when a theft does not include a complete set

The smaller the data element, the more effective this type of test, so it is most often used for 3-digit Card Verification Values. Random values are declined until the right one is guessed

Almost always used to determine CVV2 and support e-comm fraud

Easier to spot and impede than Account Testing by using velocity monitoring (limit declines, limit CVV2 per PAN)

Account Testing

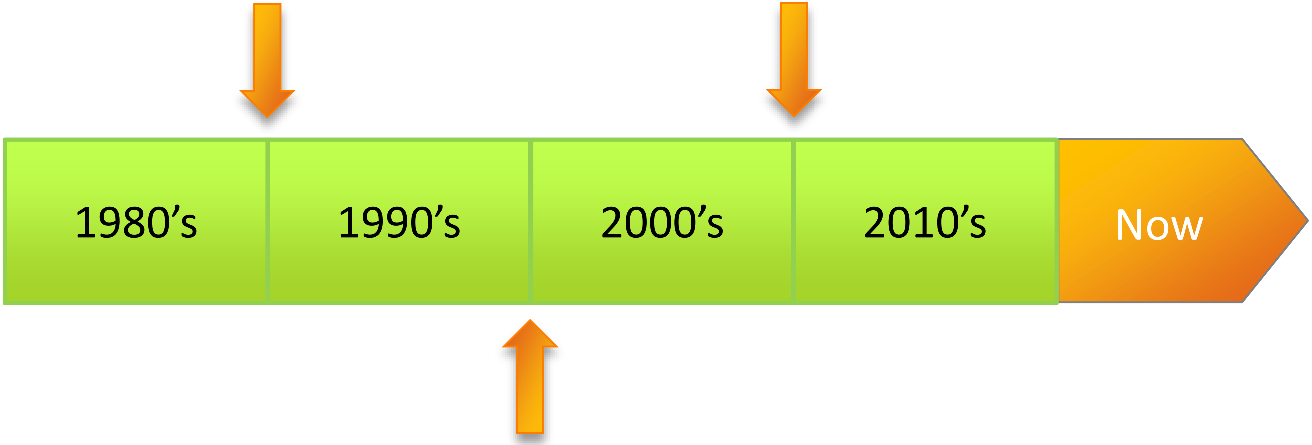
Used to verify that stolen accounts are active, this is usually one authorization per account, rarely more than two, and never ten. Large batches of accounts are often tested together

Far more authorizations are approved during account testing, but it is still 15-30%, so velocity monitoring may be linked to the merchant , POS terminal, or e-comm portal, and set above a baseline for peak volume

Many declined authorizations result in subsequent fraud, because the testers are also trying to determine whether an issuer has gaps in their risk model

One of the last steps before a stolen card is sold and used to commit fraud

The Evolution of Testing



Testing was done at payphones in an era when authorizations were verbal.

Any computer with a valid terminal ID (8 digits) can run a script that sends authorization requests for stolen account numbers to a processor gateway.

1980’s

1990’s

2000’s

2010’s

Now

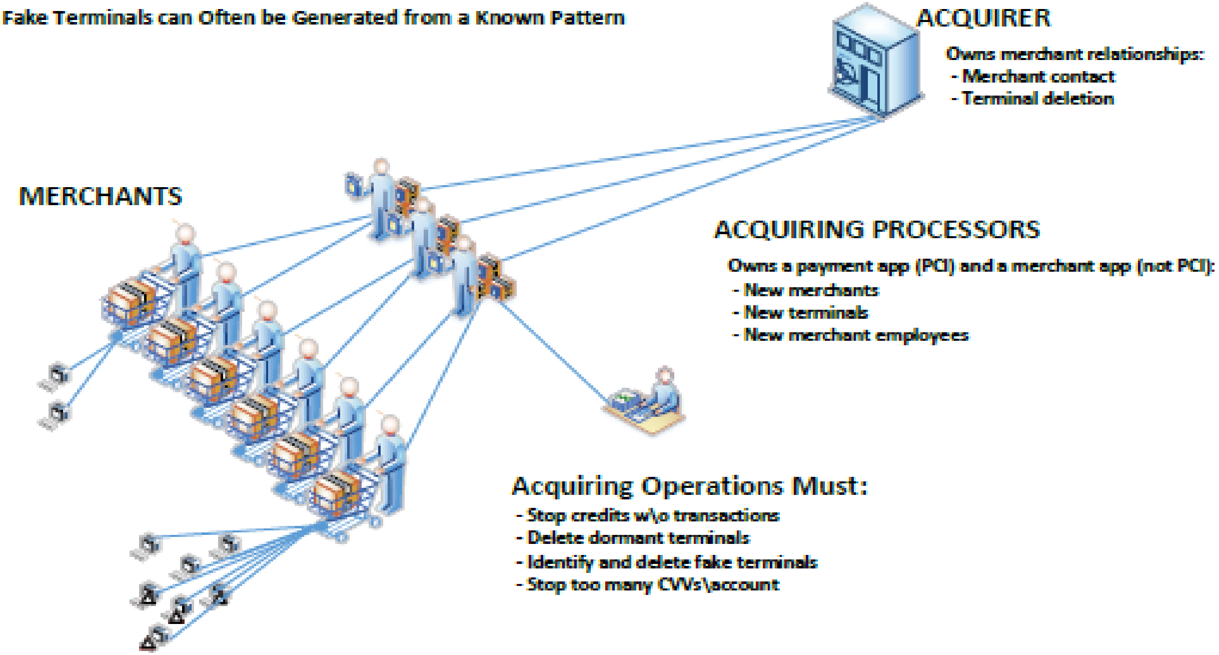
Authorizations were sent through stolen (“ghost”) terminals that dialed into a modem pool at the processor.

The volume of stolen card data on the black market has kept testing alive. Testing is no longer the key to creating a counterfeit card, but to defining its value.

Testing Facilitated Through Fake Merchant IDs

Merchant administration systems are not part of the PCI Environment

- **Fake Terminals are Common**
- **Fake Terminals can Often be Generated from a Known Pattern**



ACQUIRER

Owns merchant relationships:
- **Merchant contact**
- **Terminal deletion**

MERCHANTS

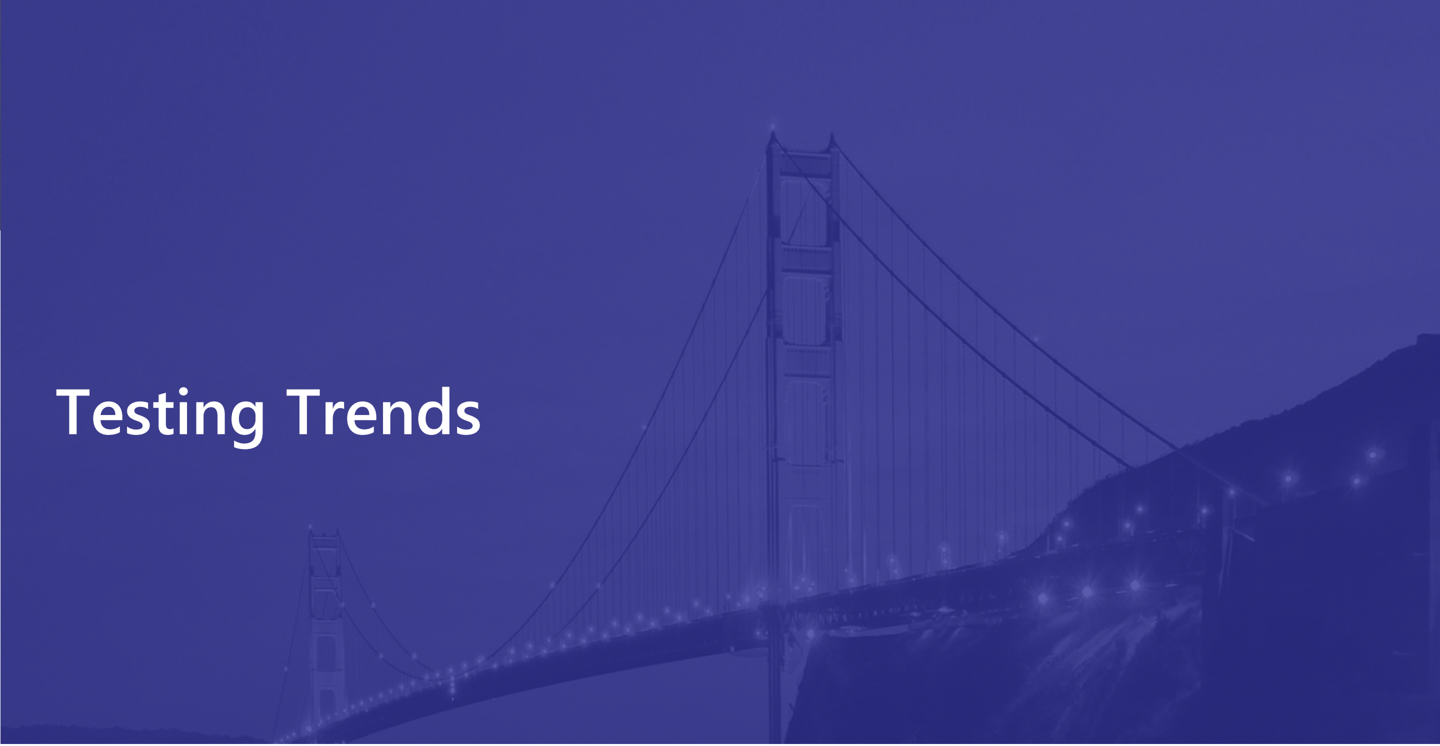
ACQUIRING PROCESSORS

Owns a payment app (PCI) and a merchant app (not PCI):
- **New merchants**
- **New terminals**
- **New merchant employees**

Acquiring Operations Must:
- **Stop credits w\o transactions**
- **Delete dormant terminals**
- **Identify and delete fake terminals**
- **Stop too many CVVs\account**

If the merchant application is poorly designed, new terminals may be assigned in a predictable sequence that is easily determined

ROOT CAUSE - FAKE TERMINALS



Testing Trends

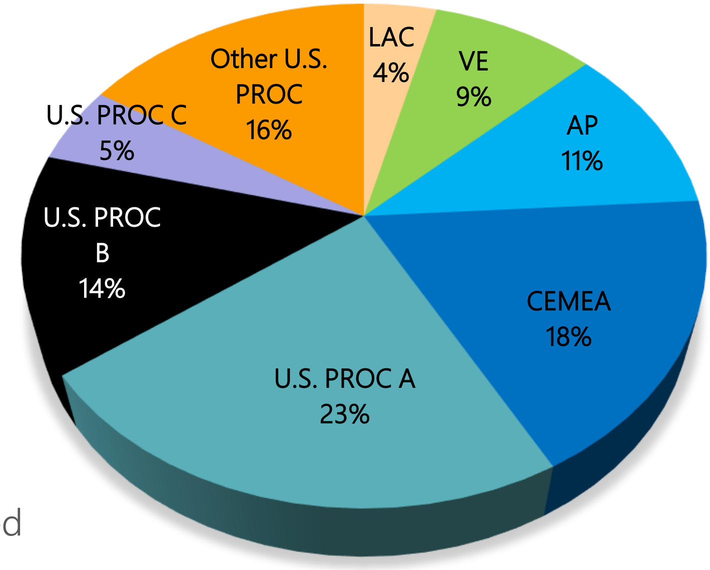
Brute Force Testing – U.S. Represents 60%

Brute force alarms between January 2015 - March 2016

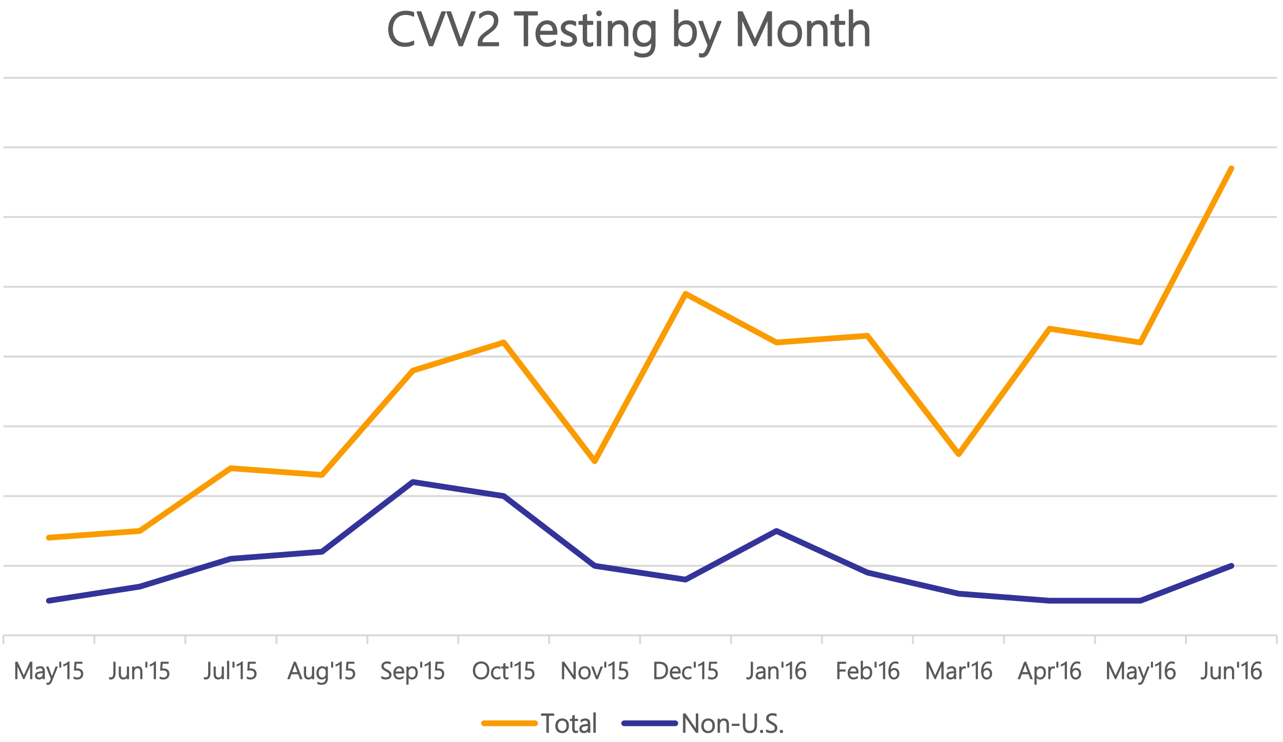
- 58% came from the U.S.
- 18% from CEMEA
- 11% from AP
- 9% from VE
- 4% from LAC

In the U.S.

- 23% came from Processor A
- 14% from Processor B
- 5% from Processor C
- 16% from Processor D-G combined

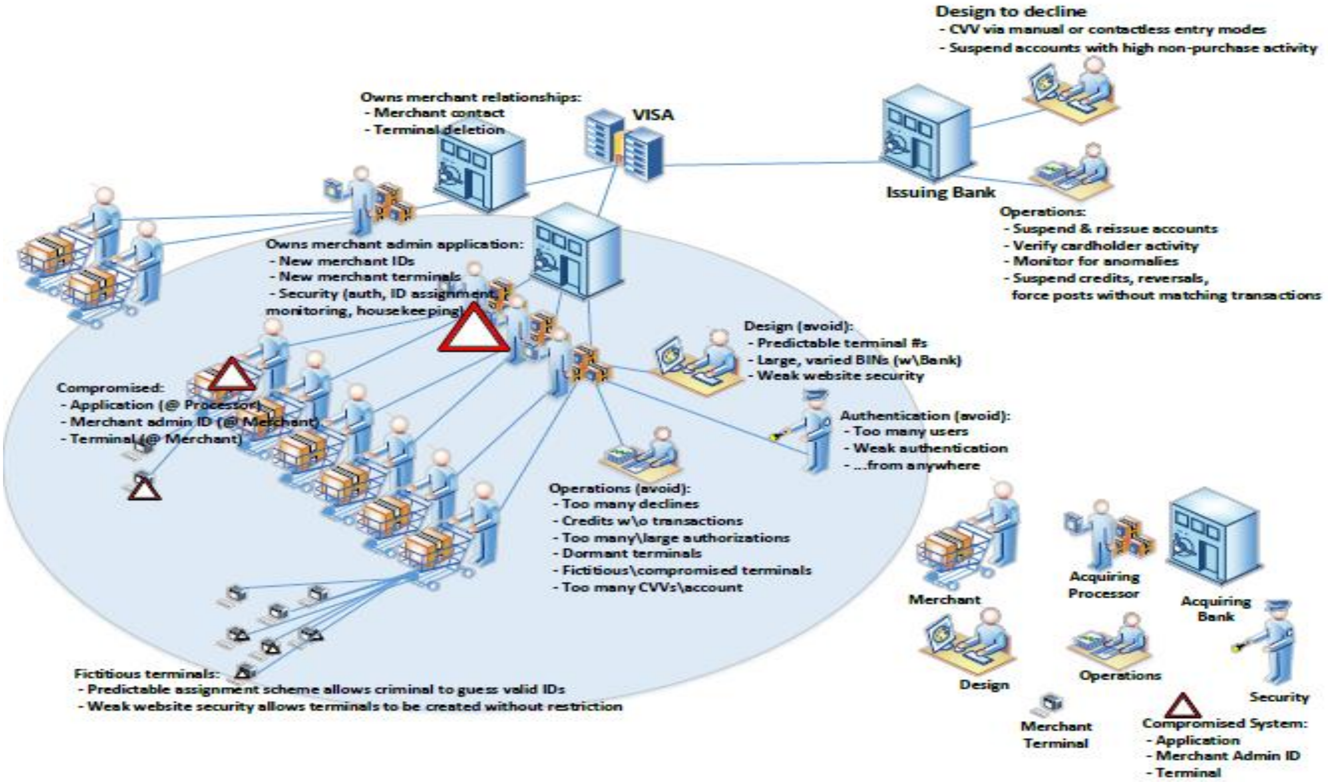


Brute Force Testing



Detecting and Responding to Testing Incidents

What Testing Looks Like to Each Party



Design to decline
- CVV via manual or contactless entry modes
- Suspend accounts with high non-purchase activity

Owns merchant relationships:
- Merchant contact
- Terminal deletion

Operations:
- Suspend & reissue accounts
- Verify cardholder activity
- Monitor for anomalies
- Suspend credits, reversals, force posts without matching transactions

Owns merchant admin application:
- New merchant IDs
- New merchant terminals
- Security (auth, ID assignment, monitoring, housekeeping)

Design (avoid):
- Predictable terminal #s
- Large, varied BINs (w\Bank)
- Weak website security

Compromised:
- Application (@ Processor)
- Merchant admin ID (@ Merchant)
- Terminal (@ Merchant)

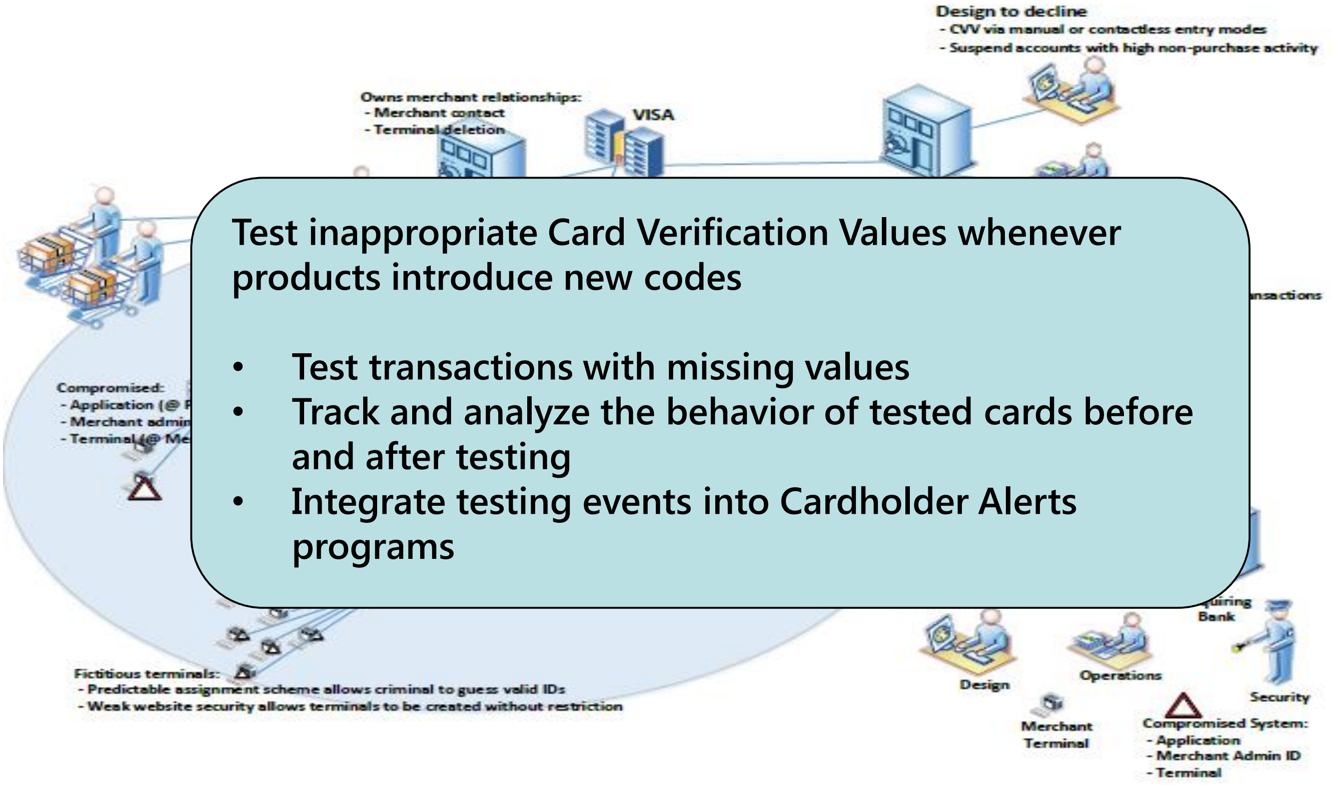
Authentication (avoid):
- Too many users
- Weak authentication
- ...from anywhere

Operations (avoid):
- Too many declines
- Credits w\o transactions
- Too many\large authorizations
- Dormant terminals
- Fictitious\compromised terminals
- Too many CVVs\account

Compromised System:
- Application
- Merchant Admin ID
- Terminal

Fictitious terminals:
- Predictable assignment scheme allows criminal to guess valid IDs
- Weak website security allows terminals to be created without restriction

Issuer Mitigation Controls



Test inappropriate Card Verification Values whenever products introduce new codes

- Test transactions with missing values
- Track and analyze the behavior of tested cards before and after testing
- Integrate testing events into Cardholder Alerts programs

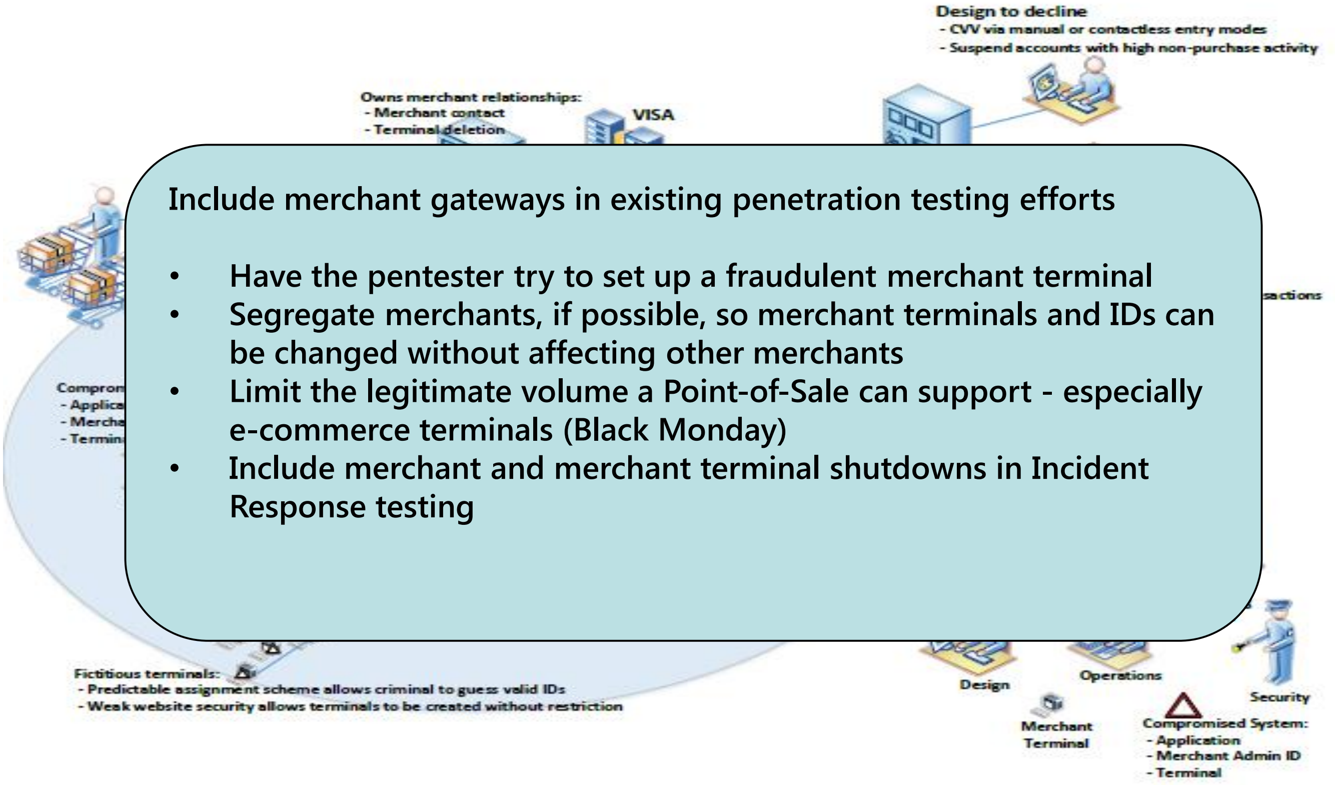
Additional Issuer Controls

- Conduct real-time velocity monitoring and notify the acquirer and brands of account testing
- Monitor Card Verification Value and block unused channels (i.e. if you do not issue contactless cards, do not permit verification via POS entry mode 07)
- Validate expiration dates for all authorizations
- Monitor authorizations by BIN for anomalies
- Investigate rapid increases of authorizations without clearing messages
- Identify and research all credits without offsetting sales
- Monitor the rate of authorization reversals at each BIN, block reversals that exceed established thresholds

Acquirer Mitigation Controls

Include merchant gateways in existing penetration testing efforts

- Have the pentester try to set up a fraudulent merchant terminal
- Segregate merchants, if possible, so merchant terminals and IDs can be changed without affecting other merchants
- Limit the legitimate volume a Point-of-Sale can support - especially e-commerce terminals (Black Monday)
- Include merchant and merchant terminal shutdowns in Incident Response testing


Design to decline
- CVV via manual or contactless entry modes
- Suspend accounts with high non-purchase activity
Owns merchant relationships:
- Merchant contact
- Terminal deletion
VISA
sactions
Comprom
- Applica
- Mercha
- Termin
Fictitious terminals:
- Predictable assignment scheme allows criminal to guess valid IDs
- Weak website security allows terminals to be created without restriction
Design
Operations
Security
Merchant Terminal
Compromised System:
- Application
- Merchant Admin ID
- Terminal

Additional Acquirer Controls

- Monitor merchants for anomalies in transactions
- Maintain strict inventory control of terminals
- Protect merchant credentials by issuing strong user IDs and passwords for payment gateway portals
- Do not print terminal or merchant ID on receipts
- Monitor velocity by account and merchant
- Investigate rapid increases of authorizations without clearing messages
- Confirm that incoming transaction data is delivered via the proper channel (e.g., dial-up versus SSL)
- Suspend and research credits without offsetting sales
- Monitor the rate of authorization reversals at each BIN, block reversals that exceed established thresholds
- Monitor testing of CVV and CVV2 thresholds to ensure individual accounts are not susceptible to brute force testing (e.g. over a handful of retries)

Communicate, Communicate, Communicate

Issuers

Develop operations contacts at acquirers that have been the targets of testing:

- Share data on losses
- Identify key resources
- Agree upon thresholds for reporting and acceptable response times for taking action

Acquirers

Convene periodic meetings between systems, security, and operations staff to review extended merchant infrastructure. Plan to:

- Plug security holes
- Upgrade and replace old systems
- If you have not been attacked, but the system is old, have a triage plan to manually identify and shut down compromised terminals

Reporting Testing Incidents

How to Report Testing Incidents to Visa

1. Confirm the issue is actual account testing and not a Common Point of Purchase (CPP) identification or recurring transaction testing
2. Requests to address chargebacks or schemes involving smaller volumes of authorization requests should be handled through standard fraud reporting, reissuing, and chargeback processes.
3. The issuer should try to contact the acquirer of record directly by using the Visa Interchange Directory contact details
4. If the VID information is not current and the issuer cannot get in touch with the acquirer to report the issue, the issuer can submit a request to Visa to report the issue to the acquirer.
5. The issuer must complete the account testing form before Risk will contact the acquirer or acquiring processor (do not send account numbers). The account testing investigation request must meet the following thresholds to be investigated by Risk:

   a) The incident of testing activity must be within the past 3 months
   b) Incidents must have more than 50 transactions attempted
   c) Incidents must have more than 10 account numbers attempted

How to Report Testing Incidents to Visa (cont.)

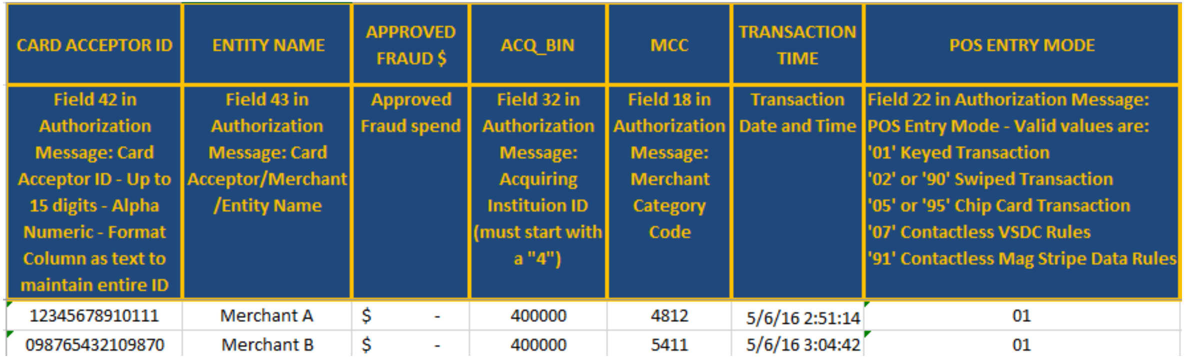
The account testing form must accompany an email providing all the following details:

- Overall duration of event (start date, peaks, end date if applicable)
- Overall number and value of fraudulent authorization attempts (assuming the file is a subset, please provide recent, monthly totals)
- Overall number of accounts tested
- Confirmed fraud losses, if any

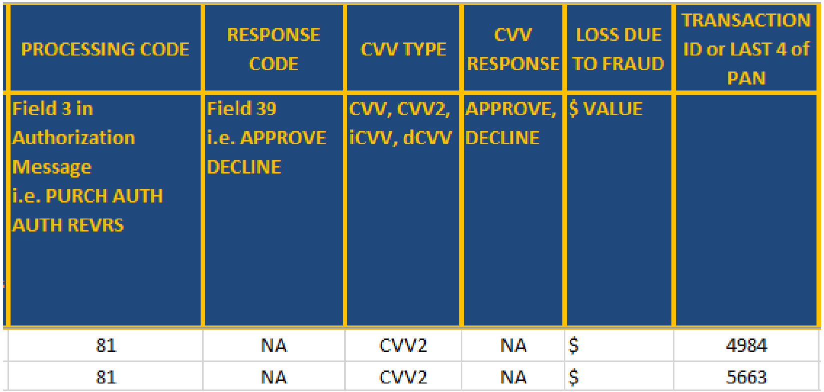
The account testing form must include all the following details:

- Card Acceptor Terminal ID (aka merchant terminal ID, field 41)
- Card Acceptor ID (aka merchant ID, field 42)
- Transaction date and time
- Issuer BIN(s)
- Acquirer BIN
- POS Entry Mode
- CVV type
- CVV approval\decline
- Authorization approval\decline\reversal

Incident Report Form



CARD ACCEPTOR ID	ENTITY NAME	APPROVED FRAUD $	ACQ_BIN	MCC	TRANSACTION TIME	POS ENTRY MODE
Field 42 in Authorization Message: Card Acceptor ID - Up to 15 digits - Alpha Numeric - Format Column as text to maintain entire ID	Field 43 in Authorization Message: Card Acceptor/Merchant /Entity Name	Approved Fraud spend	Field 32 in Authorization Message: Acquiring Instituion ID (must start with a "4")	Field 18 in Authorization Message: Merchant Category Code	Transaction Date and Time	Field 22 in Authorization Message: POS Entry Mode - Valid values are: '01' Keyed Transaction '02' or '90' Swiped Transaction '05' or '95' Chip Card Transaction '07' Contactless VSDC Rules '91' Contactless Mag Stripe Data Rules
12345678910111	Merchant A	$ -	400000	4812	5/6/16 2:51:14	01
098765432109870	Merchant B	$ -	400000	5411	5/6/16 3:04:42	01



PROCESSING CODE	RESPONSE CODE	CVV TYPE	CVV RESPONSE	LOSS DUE TO FRAUD	TRANSACTION ID or LAST 4 of PAN
Field 3 in Authorization Message i.e. PURCH AUTH AUTH REVRS	Field 39 i.e. APPROVE DECLINE	CVV, CVV2, iCVV, dCVV	APPROVE, DECLINE	$ VALUE	
81	NA	CVV2	NA	$	4984
81	NA	CVV2	NA	$	5663

Forms should be submitted to USFraudControl@visa.com

Key Takeaways

- Criminals use testing to establish the value of stolen cardholder data or randomly generated accounts
- Two types of testing – Brute Force attacks, Account Testing
- Weak merchant authentication or provisioning can be exploited
- The majority of testing occurs with U.S. acquiring processors
- Issuers can use real-time velocity monitoring to identify testing; review for authorization anomalies
- Have stronger merchant / terminal provisioning processes in place; implement velocity monitoring by account and merchant, implement thresholds for CVV2 attempts
- Issuers need to develop operations contacts with acquirers to quickly communicate testing incidents
- If reporting testing incidents to Visa, ensure all thresholds are met and relevant details are provided

Upcoming Events and Resources

Resources

- 13 August 2015 VBN – Clients Must Actively Prevent Fraudulent Credits
- 23 June 2016 VBN – How to Protect the Visa Payment System From Fraudulent Authorizations

Visa Data Security Website – www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

PCI Security Standards Council Website – www.pcissc.org

- Data Security Standards – PCI DSS, PA-DSS, PTS
- Programs – ASV, ISA, PA-QSA, PFI, PTS, QSA, QIR, PCIP, and P2PE
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more…

Questions?