



Weights and Measures/Enforcement Division
(WAM-ED)

Part 2: Commerce Skimmer Program

Goals of This Training

- Understand ways to deter installation of skimmers
- Understand components of an inspection program
- Know how to respond if a skimming device is discovered

Station Responsibility

- Stations bear brunt of the responsibility for protecting credit card information
 - Mandated to protect credit card information
 - How that is achieved is up to them
- W&M & Police can offer suggestions and ideas only
 - Walk through and discussion
 - Brochure
 - Website
 - <http://mn.gov/commerce/industries/retailers/card-skimmers.jsp>
 - List_serv

Chip Technology Protects

- *Encrypted* live communication between credit card company and card at retail location
 - Random code exchanged to verify this is a legitimate card
 - Even if card number is stolen, no ability to generate the new random code.
- Card is still vulnerable if used online or swiped at a reader which doesn't have chip technology

Chip Technology = Financial Protection Not Having Chip Technology = Liability

- 9 U.S. payment card networks have shifted liability for fraud to merchants who have not activated Europay Mastercard Visa (EMV) chip technology by October 1, 2015.
 - Accel
 - American Express
 - China UnionPay
 - Discover
 - MasterCard
 - NYCE Payments Network
 - SHAZAM Network
 - STAR Network
 - Visa
- Gas Pumps and ATM's have until October 1, 2017

<http://www.creditcards.com/credit-card-news/understanding-EMV-fraud-liability-shift-1271.php>

<http://www.creditcards.com/credit-card-news/understanding-EMV-fraud-liability-shift-1271.php>

EMV card fraud liability: Who's responsible?

Fraud scenario:	Merchant/Acquirer	Card issuer
Chip card is stolen and swiped by fraudster in store not EMV-ready.	X (If the card is PIN-based and from American Express, Discover or MasterCard)	X (If the card is a Visa, Accel, China UnionPay, NYCE or STAR Network card – no change from how this situation is currently handled)
Stolen card number is used online.		X
Chip card swiped at non-EMV compliant merchant, mag stripe data stolen and fraud occurs.	X	
Chip card-less consumer gets hit by fraud because they couldn't dip a chip card at an EMV-ready retailer.		X
Stolen/lost chip card dipped by fraudster at EMV-ready merchant.		X
Mag stripe data copied from chip card onto counterfeit card and swiped by fraudster at non-EMV compliant merchant.	X	
Mag stripe data copied from chip card onto counterfeit card and swiped by fraudster at EMV compliant merchant.		X
Chip card dipped at EMV-compliant merchant.		X

Ways to Deter and Detect before Chip Technology Installed

- Find out if your card readers can be encrypted
- Change the locks on dispensers
 - Unique keys
 - Beefier latches
- Control who has access to dispenser keys
- Talk to your service company
 - Internal alarms if cabinet is opened
 - Power down if cable to card reader is interrupted
 - Shields installed to prevent access to boards

Use Cameras

- Make sure you capture all dispensers
 - Some criminals like the far pumps because of less risk when installing
 - Some criminals willing to take a risk for bigger payoff at busier pumps
- Consider using internal cameras
 - Motion activated when dispensers are opened

Tamper Tape

- Personalized
- Serialized
- Void if tampered with
- Place it strategically
 - Over opening to access boards (not on hinge side!)
 - Over outside of scanner
- Checked daily (or even every shift)
 - Don't have it be the same person every time
 - Keep a log
 - Consequences if checks are not done
- Checked after contractors

Issues with these seals?

Tamper-evident seals



Monitoring is Forever

- Skimmers can be installed anytime
- Build a detection system
 - All employees trained
 - Serial numbers tracked
 - Daily inspections
 - Ability to detect if daily inspection not done
 - Consequences if daily inspection not done
- Sign up for list_serv and stay on top of developments
[http://mn.gov/commerce/industries/retailers/
card-skimmers.jsp](http://mn.gov/commerce/industries/retailers/card-skimmers.jsp)

Local Law Enforcement Programs

SkimStop Program

- Meet with local police to determine no current skimmers
- Place tamper tape on devices
- Check pumps every 24 hours for tampering
- 24 hour logs available upon request to document daily inspections
- Eagan Police check annually
- Skim Stop Stickers issued to let consumers know station is participating in the program

W&M + E.D. = Dynamic Duo

- **Weights and Measures uses authority under chapter 239 to:**
 - Inspect
 - Seize without warrant
- **Enforcement Division**
 - Coordinates with local law enforcement
 - Ensures seized devices are properly handled as evidence
 - Coordinates between agencies to capture rings operating in multiple jurisdictions

State Enforcement Division

- Coordinates with local law enforcement
- Local law enforcement and/or Enforcement Division staff arrive at scene to collect device on behalf of W&M
- Acts as liaison between agencies when rings operating across jurisdictions
- Alternative would be to deal with each local police agency

Phase One: Initial 4 Week Sweep

- March 7- April 1 WM investigators looked for skimmers
- Found 9 skimmers
 - Older dispensers
 - Some unmanned cardtrolls
 - Metro and southern MN

Phase Two: All Future Pump Inspections

- Routine Inspections
- Complaints
- Re-inspections



What We Look For

- Look for evidence of forced entry into dispenser
 - Broken or missing or voided tamper tape
 - Bent cabinets that look like they have been pried open
 - Broken locks or locks with tool marks and scratches
- Take pictures and note in inspection notes even if no device found

What We Look For

- Look for external credit card skimmer
- Wear gloves!
- Photograph and note on inspection
- Bag and keep in your possession until law enforcement arrives



What We Look For

Also be on the look-out for:



Keypad overlay skimmers



Hidden cameras

When a Skimmer is Found

- Make sure it really is a skimmer
 - May need service company confirmation
 - Touch as little as possible
 - Wear gloves
- Secure dispenser from further use
 - Block with truck/cones/bag-on-handle or power down unit
 - Don't touch other than to re-close cabinet until police arrive
- Secure all video footage
- Be aware that an employee or a contractor may be involved. Follow law enforcement instructions on whether you discuss what you find with station personnel.

Other Notes

- Document any discussion relating to credit cards
 - Has anyone contacted the station about suspicious activity related to their credit or debit card?
 - If so, get the caller's complete contact information (name, address, phone number, type of credit card) and the details of the allegations.
 - Does the station have video?
 - If anything is suspicious, the station should make a copy of any video it has concerning the matter and give the video to law enforcement or the Fraud Bureau as soon as possible.
 - Have employees noticed any suspicious people or activity?

Questions?

- Contact Information

Julie Quinn, Director

Minnesota Department of Commerce

Weights & Measures Division

651-539-1556

Julie.Quinn@state.mn.us