

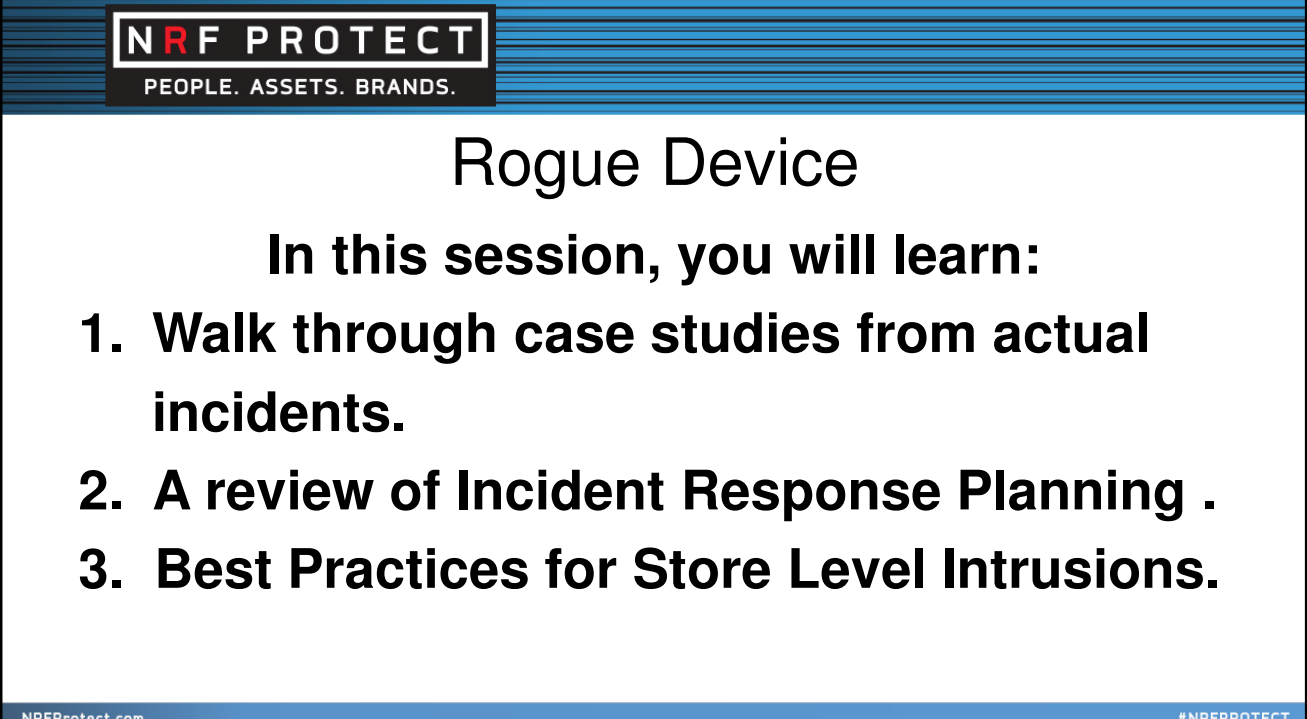
NRF PROTECT
PEOPLE. ASSETS. BRANDS.

Rogue Device

What To Do When you Get the Call

NRF NATIONAL RETAIL FEDERATION

#NRFPROTECT



NRF PROTECT
PEOPLE. ASSETS. BRANDS.

Rogue Device

In this session, you will learn:

- 1. Walk through case studies from actual incidents.**
- 2. A review of Incident Response Planning .**
- 3. Best Practices for Store Level Intrusions.**

NRFProtect.com #NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

WILLIAMS-SONOMA, INC.

Williams-Sonoma • Pottery Barn • Pottery Barn Kids • West Elm • PBTeen
Williams-Sonoma Home • Rejuvenation • Mark and Graham

The Numbers

\$4.68 - \$4.73 Billion • 612 Stores
Multiple ecomm Websites • Direct Mail Catalogs

Locations

United States • Canada • Australia • United Kingdom
International Shipping Worldwide

Franchises

Bahrain • Dubai • Kuwait • Abu Dhabi • Lebanon
Philippines • Mexico City



NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

YEAR IN REVIEW OF BREACHES

JAN

Xoom \$31 million business email compromise

FEB

Deep Panda likely cause of Anthem breach estimated 1/3 of Americans affected

MAR

Premera (Blue Cross) breach affecting 11 million people

APR

Great Cannon DDoS attacks on GitHub, GreatFire

MAY

Healthcare Data breaches cause problems for insurance providers

JUN

OPM breach – 21 million (and counting) victims

JUL

Harvard, Penn State, Trump Hotels, UCLA, Hacking Team and Ashley Madison

AUG

American Airlines; US DoD; USDHHS; IRS; Ubiquity \$47 millions loss

SEP

Blue Termite Chinese cyber-espionage attack on Japanese companies

OCT

Experion breach affects 15 million customers; Patreon; Scottrade

NOV

Dridex banking malware; Vtech; 70 Million US Prison calls; FEB Law Enforcement Portal

DEC

Black Energy malware causes power outages in Ukraine

Source: Verizon 2016 Data Breach Investigation Report

NRFProtect.com

#NRFPROTECT

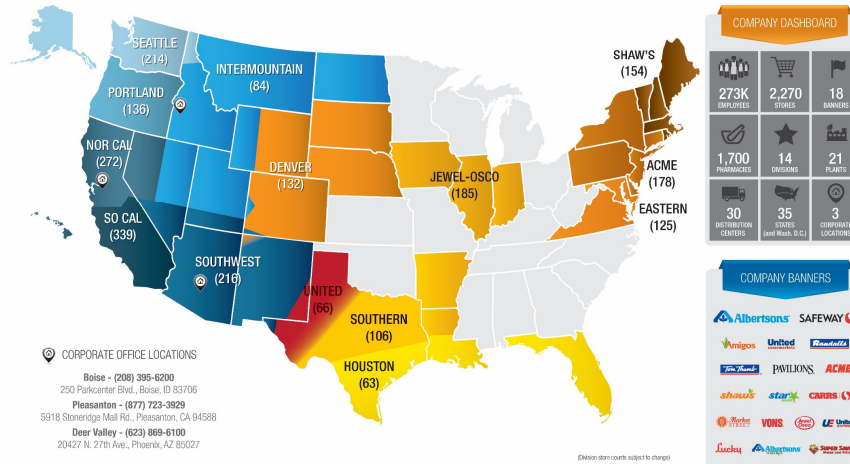
NRF PROTECT

PEOPLE. ASSETS. BRANDS.



Our favorite local supermarkets™ from coast to coast

FEBRUARY 2016



NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Case Study II

- Store identified a skimmer on a self checkout register
- Store personnel removed device and placed in a bag, then contacted Asset Protection
- Alert was sent out to other District stores
- Based on alert, another store confirmed finding a skimmer located within 10 miles of other store
- Asset Protection responded to both stores, confirmed compromise, and provided evidence to Department of Homeland Security

NRFProtect.com

#NRFPROTECT

NRF PROTECT
PEOPLE. ASSETS. BRANDS.



Related Coverage

Thieves Use Skimmers at Peninsula ATMs

Police warn Marin County residents of threatening text message scam

Union City police warn residents of IRS scam

Marina District.

Shortly after using his card at the Safeway, he received an email from his bank warning him of a potentially fraudulent charge.

A Safeway employee confirmed that two stores in the Bay Area had reported credit card thefts. Safeway said they will release a statement at some point on Wednesday with the stores affected.

Some customers who had their account information stolen say that their entire bank accounts were drained.

SAN FRANCISCO (KRON) – Residents are being warned of credit card scams at several Safeway grocery stores in the Bay Area Wednesday morning.

Safeway is investigating the discovery of the card readers that thieves use to steal bank account and pin numbers.

A KRON4 employee had their card information stolen Wednesday morning from the Safeway in San Francisco's

NRF PROTECT
PEOPLE. ASSETS. BRANDS.

Safeway has issued a statement about the skimmers:

“ Today’s online story regarding skimmers at Safeway stores does not reflect that these rare discoveries were made during our own routine inspections, nor does it convey that these are isolated incidents. It is important for customers to know that no credit or debit card data was compromised by the two skimmers that were discovered at our Dublin Boulevard store in Dublin and the Bancroft store in Walnut Creek in September. (Reports regarding stores in Castro Valley and Menlo Park are inaccurate.) No skimmers have been discovered since that time. Like all responsible business owners, our store teams routinely inspect all point of sale devices and discovered the two skimmers during these inspections.

When our store teams find evidence of criminal activity like this, we have been able to pinpoint with surveillance video when the devices were installed and how many transactions were processed. We immediately followed the proper protocol of contacting law enforcement and the banks that service the few cards that were used on those pin pads. Customers who have any concerns, should review their bank statements for fraudulent activity in the September/October timeframe, or contact their cardholder or bank directly.

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Case Study II Conclusion

- In cooperation with DHS, Suspect pictures were disseminated to the public
- No account numbers were compromised (devices were not blue-tooth enabled)
- Suspect later identified by Safeway employee who observed the DHS release of information
- Case is currently under investigation

NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Lessons Learned

- Timeliness and accurate reporting of incident facts crucial to decision making and communication within and outside of organization
- Take time to evaluate scope and impact
- Relationship and partnership with Law Enforcement critical in outcome
- Key partners with Banking and processors assist in quick determination of impact to organization
- Communication within organization to follow established rules constantly reinforced and reviewed

NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.



FRONT



SKIMMING MECHANISM



BACK



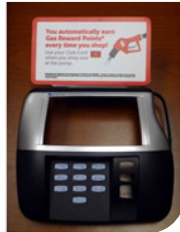
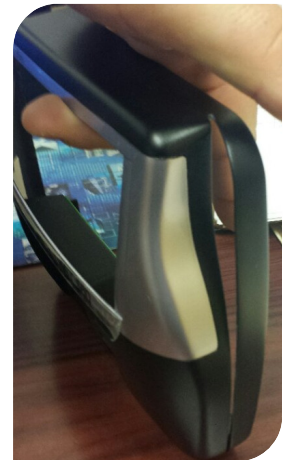
REUSED SAFEWAY STICKER

NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

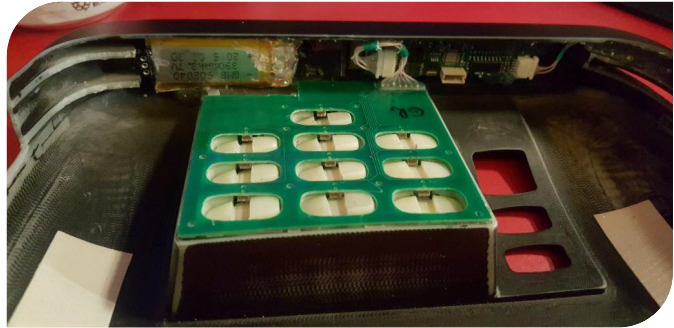


NRFProtect.com

#NRFPROTECT

NRF PROTECT
PEOPLE. ASSETS. BRANDS.

Interior View Of Skimmers



NRFProtect.com

#NRFPROTECT

NRF PROTECT
PEOPLE. ASSETS. BRANDS.



REAL



FAKE



NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Types of Skimming Devices Fuel Pumps

- Interior: the majority of gas pump skimmers are installed inside the pump
- Exterior mounted skimmer (false card reader) placed over legitimate reader
- Some are Blue Tooth enabled (can retrieve data from a short distance without being physically connected to the device)
- New skimmers on the market are embedded in the card readers and the crooks replace the entire card reader. (this can be done in literally seconds by a skilled criminal.)
- Hi-tech pinhole cameras concealed in a brochure holder & attached next to the pump will capture the card holder's PIN

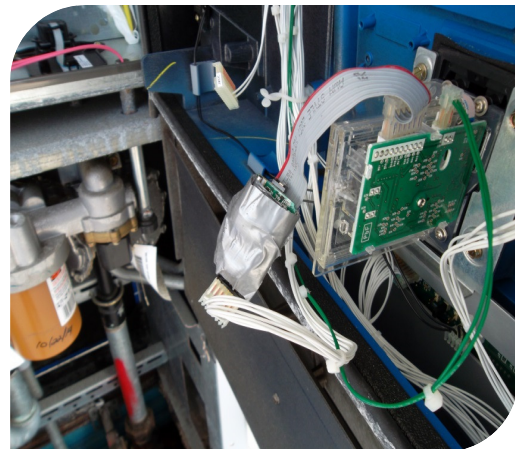
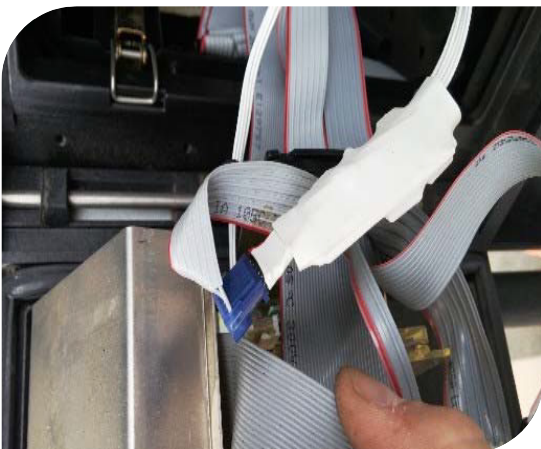
NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Interior Skimmer Examples



NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Exterior Mounted



NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

New Generation Internal Skimmer “Shimmer”

- Super thin, .1mm thick, card reader that slides right into the card slot.
- They use a carrier card to insert the device.
- This shimmer is designed to pull credit information from the chip embedded in the newer credit cards instead of the magnetic strip. Blue tooth enabled.

NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

“Shimmer”

- This new skimmer is paper thin & runs off of a lithium coin battery. It is thin enough to fit into the card reader’s “throat”.



NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Incident Response – Now What? Managing the Compromise...

NRFProtect.com

#NRFPROTECT



Incident Response Process Flow



- | | |
|--|--|
| <p>1 →</p> <ul style="list-style-type: none"> Continuous improvement on Security Operational Controls, Standards and Policy. Review and Rehearse IR Plan, Make needed adjustments where necessary. | <p>4 →</p> <ul style="list-style-type: none"> Prior to Containment & Eradication, if possible, secure and collect evidence. Perform analysis to better understand the nature of the threat. A higher degree of successful elimination. |
| <p>2 →</p> <ul style="list-style-type: none"> An Incident - <i>Any unlawful, unauthorized or unacceptable action involving a computer system or network.</i> Defined Incident Categories 0 – 6. Incident Severity – 1, 2 or 3. | <p>5 →</p> <ul style="list-style-type: none"> Once the root cause of the incident is eradicated; <ul style="list-style-type: none"> Correct the vulnerability. Restore operations back to normal. |
| <p>3 →</p> <ul style="list-style-type: none"> Established and defined containment and eradication measures per operational support area to minimize damage and prevent additional damage. Understand business impacts and communicate accordingly. | <p>6 →</p> <ul style="list-style-type: none"> Assessing and documenting incident response activities; <ul style="list-style-type: none"> Conduct post-mortem reviews. Report KPIs. |



Step 1: Planning and Preparation

“An ounce of prevention is worth a pound of cure.”

- Benjamin Franklin

Having a Formal Incident Management Plan is the First Step to Ensure an Effective Incident Response.

Key Focus Areas:

1. Building a solid relationship with your Information Security team.
2. Identifying who are the key stakeholders in the Incident Management process.
3. Communicate and socialize response procedures to both IM stakeholders and associates.
4. Practice, practice, practice.
5. Incident Response Planning requires continuous improvement.
 - Avoid the Ronco approach of “set it and forget it.”



NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Step 2: Detection and Classification

Initial Notification: An associate finds a suspicious device attached to the POS.

Now What?

Scoping and Discovery:

1. Do not take action on your own.
 - Fight human nature to remove the device as this could tamper with evidence as well as tip off the attacker.
2. Trigger your Incident Management plan.
 - All associates need to understand what to do and who to call.
3. Assess what's at-risk or what has been compromised
 - Determine points of data egress
 - Scan the enterprise for like compromised behavior
4. Classify the Incident
 - Isolated incident? High, Medium or Low? Protected data involved?
 - Setting the appropriate response. Handle internally or call for assistance?



NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Step 3: Containment and Eradication

Containment: Taking the right steps to “stop the bleeding.”

Eradiation: Preventing further compromises.

So, What's Next?

Containing the Incident:

1. Work with Security to capture POS activities
 - Capture activity logs, OS, running software and firewalls.
2. Work with Security and Network teams to isolate the compromised environment.
 - Take the POS system off the network.
 - Ideally, have a dedicated security network segment where you can move the affected system without disabling the port.

Other Considerations:

1. Dependent system impacts and business continuity concerns.
2. Who is accountable and authorized to make this decision.



NRFProtect.com

#NRFPROTECT

Step 4: Collection and Analysis



Collect evidence for follow-on analysis.

Why is this Important?

Taking the time to perform further analysis leads to a better understanding of the threat and increases your chances to eliminate it.

Considerations:

1. Establish criteria to whether to use your internal forensics team or a forensics service provider.
2. Ensure you use forensically sound procedures;
 - Repeatable
 - Well documented
 - Least intrusive to the affected system
 - User proper evidence handling procedures
3. Analysis and root cause;
 - Who and how many associates were impacted?
 - Status of the incident (nature & location)

Evidence Chain of Custody	
Released By:	Received By:
Name / Title:	Name / Title:
Signature:	Signature:
Date / Time:	Reason:
Released By:	Received By:
Name / Title:	Name / Title:
Signature:	Signature:
Date / Time:	Reason:
Released By:	Received By:
Name / Title:	Name / Title:
Signature:	Signature:
Date / Time:	Reason:

Step 5: Remediation and Recovery



Identify changes that might be necessary to ensure containment is effective and eradication is thorough.

Your Goal: Return to normal operational state.

Once you have root cause of the incident has been eradicated:

1. Correct any vulnerabilities that contributed to the incident.
2. Accomplish all recover tasks to restore normal operations.

Incident Recovery:

1. Replace POS sled or reinstate original once forensics has been completed and the device is recertified for service by equipment manufacturer.
2. Rebuild POS system with a certified image.
3. Establish new protocols around “tamper testing” POS devices.



Step 6: Assessment and Documentation



Once your operations have returned to normal state.....

Conduct a Lessons Learned Session with your IM Stakeholders:

- What went right?
- What went wrong?
- What could be improved?

Considerations:

1. Your post-mortem session;
 - Be timely, within 3 business days after incident resolution
 - Assign a scribe or note taker to capture session details
 - Distribute and retain results for future references
2. Capture KPIs to capture time, cost and damage.
3. Capture incident as a future "Mock Incident Scenario."
 - Capture output of training to further enhance your IM plan

Category	Measurement	Description
Incidents	# Incidents / Year	Total number of incidents per year
	# Incidents by Type / Year	Total number of incidents by category per year
Time	# Hours / Incident	Total number of personnel hours resolving incident
	# Days / Incident	Total number of days spent resolving incident
Cost	Monetary Cost / Incident	Total estimated monetary cost per incident, to include containment, eradication, remediation, and recovery, as well as collection and analysis activities (this may include labor costs, external entity assistance, tool procurements, travel, etc.)
Damage	# Systems Affected / Incident	Total number of systems affected per incident



To recap on today's takeaways...

- Assure strong IT and LP partnerships.
- Make sure you have a current Incident Response Plan.
- Practice & rehearse the Incident Response Plan so it is second nature.
- Train stores on clear expectations and key contacts when an incident occurs.

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Rick Lloyd
Director Information Security
Williams-Sonoma, Inc.
(916) 626-5867
relloyd@wsgc.com

Jason Griffin
Corporate Asset Protection Manager
Albertsons Companies
(503) 806-2448
jason.griffin@safeway.com

Gail Morris
Director LP – Corporate & Direct
to Consumer
Williams-Sonoma, Inc.
(415) 816-5505
gmorris@wsgc.com

NRFProtect.com

#NRFPROTECT

NRF PROTECT

PEOPLE. ASSETS. BRANDS.

Rate This Session

For each unique session evaluation, NRF will donate \$1 to LP Foundation!

1. Log into Mobile App

Username = Last Name

Password = Registration ID on badge

2. Find session in schedule

Feedback form is on session details screen

NRFProtect.com

#NRFPROTECT