



Hannaford School of Hard Knocks

While there's no cure-all to data theft, the case offers insight to strengthening the industry as a whole

By Tom Wright

News of stolen or compromised consumer data seems to break so often, it's easy to overlook the implications on the electronic payments industry. Yet the Hannaford case stands out from others because the Scarborough, Maine-based supermarket chain's breach appears to represent a new line of attack: the first large-scale piracy of card data while the information was in transit. And, more important to payments professionals, this theft of up to 4.2 million credit and debit card numbers marks the first time a PCI-compliant company was compromised.

"Thieves commonly pilfer payment card data sitting in databases maintained by merchants or card processors because it's low-hanging fruit," says Neil Weicher, president of NetLib, a database encryption software developer in Stamford, Connecticut. "It takes a high level of technical skill to write programs that can intercept data in transit."

The malware recorded the data stored on the magnetic stripe on customers' cards as they used them at the checkout counter. This data allows criminals to recreate the actual card and conduct fraud much more easily. With full magnetic stripe data in hand, they are no longer limited to perpetrating fraud over the Internet.

Compliance Matters

The Hannaford case prompted a litany of complex legal discussions and numerous customer lawsuits. The biggest point of contention is whether the company was actually compliant at the time of the breach. The PCI Data Security Standard currently does not require data that's traversing a private, wired local area network (LAN) to be encrypted. It only requires encryption of sensitive information traveling across an open network, usually the Internet or a wireless network.

"If Hannaford is found to not have



been in PCI compliance at the time of the breach, the bank and credit union issuers are more likely to sue to recover their costs for re-issuing cards and notifying consumers," says David Navetta, president of InfoSecCompliance LLC in Denver. He adds that "even if it was compliant, there are many complex factors that will come into play in this case."

The PCI mandate implies that PCI-compliant businesses do not have to bear the financial burden of fraud resulting from criminals using cards obtained through a known data breach. However, it stops short of answering more detailed questions, such as:

- If the acquiring bank is fined, will it be able to recoup the cost from Hannaford?
- If a Qualified Security Assessor (QSA) certifies a merchant as PCI compliant and later that merchant's system is compromised, is the QSA liable in any way?
- Will the courts give Hannaford credit for due diligence if it was PCI compliant at the time of the breach, or will they deem that "reasonable controls" above and beyond PCI compliance should have been in place?
- Is it possible to be PCI compliant and

still have "unreasonable security" for purposes of a negligence suit by consumers or issuers?

Considering all of these difficult questions, some legal observers believe that the Hannaford case may end up being a seminal one that casts light on how PCI compliance plays out in a real-world situation.

Fortifying Defenses

As the case works its way through the legal system, many security experts recommend companies start a campaign to strengthen their defenses now.

"We all should bear in mind that PCI represents the lowest common denominator of security," says Slavik Markovich, chief technology officer with Sentrigo in Woburn, Massachusetts. "Making PCI requirements more stringent will not prevent breaches from occurring, but we must remember that being PCI compliant almost always means that the organization is more secure than it was before being compliant."

Jarrett Kolthoff, a former Army counterintelligence agent and co-founder of SpearTip Technologies, has a somewhat harsher view of PCI: "All too often PCI is

just checking off boxes on a form, and no true penetration testing is taking place,” he says. “Adherence to standards is simply not enough. Companies must have proactive security measures in place, have visibility into their networks with a protocol analyzer and SIM (security information management) system, and, most importantly, have the human element in place to diligently monitor and correctly analyze what these systems are reporting.”

So what systems and tools should merchants have in place? “It is a pretty safe bet that there was no IPS (intrusion prevention system) installed at Hannaford,” suggests Ken Pappas, a security strategist at Top Layer Networks. And Markovich adds that “we don’t know the full details of the breach, but from the available information, it seems as though an IPS/IDS (intrusion detection system) would have alerted on the unusual traffic of the stolen credit cards to an unauthorized location. White list addresses on both the firewall and in the IPS/IDS would have definitely helped.”

Meanwhile, other security experts are

touting the rapidly growing arena of data leak prevention (DLP) products, which can help organizations protect against the loss of sensitive data.

Some people in the industry also are lobbying for end-to-end encryption. Pappas, however, claims that “encryption is a great idea, but there is no industry standard in place that would make it feasible to implement end-to-end encryption over various systems.”

“There is no real architecture in place that facilitates end-to-end encryption,” agrees David Wren, CEO of SpearTip Technologies. “In fact, there is no silver bullet for securing sensitive systems, and encryption is not a cure-all. Overall, the best approach to security is a layered methodology.”

Family Dollar Stores has more faith that encryption is a viable defense. The discount store chain recently partnered with VeriFone to roll out its new VeriShield Protect card data security program. Developed in conjunction with Semtek Innovative Solutions, VeriShield Protect shields credit and debit account information from the instant a card is

swiped until the data is received at a secure decryption appliance located in a merchant’s secure data center, which is at an off-site service provider or an acquirer or processor organization.

The system’s technology, H-TDES (Hidden-Triple Data Encryption Standard), encrypts the personal account number and magnetic-stripe data in a manner that other applications interpret as valid card data, explains Patrick Hazel, CEO of Semtek.

Even with such cutting-edge security applications in place, you can’t ignore the human element. “Social engineering tactics were quite popular years ago, and are now making a strong comeback,” says Jim Stickle, chief technology officer for TraceSecurity. “The value of a properly implemented security awareness program can be tremendous—for a fairly low investment, an organization can reap big rewards by preventing security breaches and incidents.” **TT**

Tom Wright is a contributing writer to Transaction Trends. Reach him at tom@cunews.com.



“When making a good impression counts”™

Count on Quality Imprinters and Merchant Plates From Data Systems.®

Email: Sales@DataSystemsCompany.com

(843) 856-1025

Do YOU Want MORE?

- More Residuals
- More Profits
- More Programs
- More Services
- More Support
- More Innovation
- More Reporting

Everything you need to be successful ... and More!

Orion Payment Systems. **More.**

Call Orion NOW!

Recurring Payments • Virtual Terminal
 Online Payment Solutions • AutoPay
 Chargeback Protection & Recovery
 Cash Advance • Check Programs
 Integrated POS • Petroleum
 Online Reporting

ORION
PAYMENT SYSTEMS

877-941-6500 sales@orionps.com www.orionps.com

Orion Payment Systems is an ISO/MSP of HSBC Bank USA, Buffalo, NY