Assigning Legal Responsibility for Corporate Account Takeover

Dan Mitchell
USM Corporate Partners
October 23, 2013
"You know, you can do this just as easily online."
Automated Teller | How cyber criminals allegedly siphoned millions of dollars out of U.S. banks

1. Criminals in Eastern Europe send seemingly innocent emails to small businesses and municipalities in the U.S.

2. These emails contain the Zeus Trojan malware. Once the emails are opened, the malware embeds itself into the victims’ computers.

3. The malware records the victims’ keystrokes, which gives the cyber criminals access to account numbers, passwords and other personal data.

4. The cyber criminal uses the information to take over the victims’ bank accounts.

5. The cyber criminal transfers money to accounts set up with fake IDs by ‘mules’—people traveling in the U.S. or in the country on student visas.

6. The mules keep a percentage of the money—typically 10%—and transfer the rest to the cyber criminals.

Source: WSJ research
Internet-Based Banking Transactions

• Wire transfers and Automated Clearing House transactions initiated on the web
  • ACH = an electronic network for the exchange of payment instructions between and among financial institutions
• Examples: Direct deposit of payroll, direct payment of bills and business-to-business payments

• In 2012, 21 billion ACH transactions worldwide, valued at $36.9 trillion
Consumer vs. Business Transactions

- Unauthorized transactions in *consumer* accounts are governed by the Electronic Fund Transfer Act, 15 U.S.C. §1693, et seq.
  - See “Regulation E” promulgated by the Federal Reserve

- Unauthorized transactions in *commercial* accounts are governed by Article 4A of the Uniform Commercial Code
  - 11 M.R.S.A. §§ 4-1201, et seq.
Business Transactions: Covered by Article 4A of the Uniform Commercial Code

- The UCC consists of recommended sets of laws promulgated by national organizations with the goal of harmonizing state laws
- Article 4A, pertaining to electronic funds transfers, was promulgated in 1989
- It subsequently was enacted in all 50 states
- It remains largely unchanged in most jurisdictions
- No substantial revisions have been proposed
UCC Article 4A

• Operates as a risk-shifting mechanism for unrecoverable losses

• A bank must show:
  1. The bank and its customer agreed that the bank would use a particular set of security procedures to verify the authenticity of payment orders
  2. The security procedures implemented by the bank were commercially reasonable
  3. The bank accepted the payment order at issue in good faith and in compliance with the agreed upon security procedures

• See UCC §4A-202(b)
Defining a “commercially reasonable” security procedure

- It’s a question of law (i.e. a judge will decide) based on the following factors:
  1. The wishes of the customer expressed to the bank
  2. The circumstances of the customer known to the bank, including the size, type and frequency of payment orders normally issued by the customer to the bank
  3. Alternative security procedures offered to the customer
  4. The security procedures in general use by customers and receiving banks similarly situated

- See UCC §4A-202(c)
Conclusions

- Look closely at your account agreement – do you understand the security procedures?
- Education/Communication/Documentation
  - Ask questions
- If you are victimized, immediately consult an expert on electronic security procedures
Privacy and Security Contract Terms in Outsourcing Agreements

Josh Silver
USM Corporate Partners
October 23, 2013
Standard Provisions

- Definitions
- Confidentiality
- Compliance with data privacy and data protection laws
- Specific data protection requirements
- Security incident reporting processes
- Indemnities, damages, liability caps/exclusions
- Third-party security audits
Definitions

Clearly define “personal information.” Other important contract provisions are tied to this definition. Examples:

• “Personal information” means any information that relates to a natural person and that could be used, either directly or indirectly, to identify such person.
• “Personal information” means any information relating to an identified individual (or an individual whose identity could be discovered based on the information) that supplier and/or supplier personnel have access to, receive, create, transmit or maintain in connection with performing services for client hereunder, including any information treated as personal information under applicable law.
• “Personal information” has the same meaning as set forth in the regulations issued by the Massachusetts Office of Consumer Affairs and Business Regulation that implement Chapter 93H of the Massachusetts General Laws codified at 209 C.M.R. Part 17.
Confidentiality

Remember to include “personal information” within the categories of information that constitute the client’s “confidential information”!
Compliance with Data Protection Laws

Obligate the service provider to comply with applicable data protection laws:

• Supplier shall not collect, handle, process, disclose, use or store any personal Information, except for performance of the services, strictly in accordance with this agreement, and only to the extent permitted or required by the data protection laws or other applicable laws.

• Client shall determine the scope, purposes, and manner for which personal information may be accessed or processed by supplier, and supplier shall limit its access to or use of personal information to that which is necessary to provide the services, comply with applicable laws, or as otherwise directed by client.

• Supplier agrees to collect, store, process, disseminate or use personal information obtained from client (i) only as expressly directed by client in writing, (ii) in accordance with the data protections laws and other applicable law, and (iii) in accordance with client’s information security and privacy policies and procedures.

• Supplier will comply with all information security requirements that apply to supplier and/or client under federal, state or other applicable law.
Specific Data Protection Requirements

Consider adding specific data protection requirements beyond compliance with data protection laws or particular standards (such as PCI-DSS):

• Implementation of security programs
• Security training programs for personnel
• Security risk assessments
• Encryption of data
• Access controls
• Computer security guidelines (including vulnerability scanning, maintenance of log files concerning activity on supplier’s computer systems, anti-virus software, etc.)
Security Incident Reporting Process

• Require the service provider to notify the client immediately upon the discovery of a breach of confidentiality involving personal information
• Consider including in the outsourcing contract a specific security incident reporting process so that there is no confusion when a breach occurs
Indemnity, Damages, Caps/Exclusions

- Consider defining specific classes of damages for which the service provider will be responsible in the event of a breach, such as notifications to affected individuals, state or federal agencies, and/or credit bureaus, credit monitoring services, identity restoration services, fraud insurance, establishment of a call center to respond to customer inquiries and/or legal and professional services fees, etc.
- Include an indemnity, not limited to third party claims, for any breaches of confidentiality or information security breaches. Carve indemnity obligations out of any disclaimer of indirect damages or general liability cap.
- If indemnity is limited to third party claims, carve out of any disclaimer of indirect damages or general liability cap, costs and liability relating to information security incidents.
- If the service provider is unwilling to remove its indemnity obligations or liability for data breaches from the general liability cap, consider a separate cap for costs relating to data breaches.
Third Party Security Audits

- Consider requiring the service provider to subject itself to a standard set of audits or specific audits (e.g., SSAE 16, PCI compliance audits, etc.)
- Require the service provider to provide the client with the reports stemming from such audits and to promptly correct any deficiencies revealed in the audits